

**ANÁLISIS, DISEÑO E IMPLEMENTACIÓN DE UNA APLICACIÓN PARA LA
INTEGRACIÓN DE REQUERIMIENTOS NO FUNCIONALES DE
AUTENTICACIÓN, AUTORIZACIÓN Y AUDITORÍA.**

**OSCAR ENRIQUE PIÑEROS OVALLE
STEPFANIE CASTILLO ESCOBAR**

**UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD INGENIERÍA DE SISTEMAS
BOGOTÁ
2016**

**ANÁLISIS, DISEÑO E IMPLEMENTACIÓN DE UNA APLICACIÓN PARA LA
INTEGRACIÓN DE REQUERIMIENTOS NO FUNCIONALES DE
AUTENTICACIÓN, AUTORIZACIÓN Y AUDITORÍA.**

**OSCAR ENRIQUE PIÑEROS OVALLE
STEPHANIE CASTILLO ESCOBAR**

ASESOR: JAIME ALBERTO CHAVARRIAGA

**UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD INGENIERÍA DE SISTEMAS
BOGOTÁ
2016**

Nota de aceptación

Firma del presidente del jurado

Firma del jurado

Bogotá, 21 Noviembre 2016

No hay secretos para el éxito, este se alcanza preparándose, trabajando
arduamente y aprendiendo del fracaso.
COLIN POWELL

Contenido

RESUMEN.....	9
INTRODUCCIÓN	10
CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA	11
1. OBJETIVOS	11
1.1.1 Objetivo General.....	11
1.1.2 Objetivos Específicos:	11
1.2 PROBLEMA.....	11
1.2.1 ANTECEDENTES.....	12
1.2.2 JUSTIFICACIÓN	14
1.2.3 ALCANCES.....	15
1.2.4 LIMITES.....	15
1.2.5 SISTEMAS DE HIPÓTESIS	16
1.2.6 SISTEMAS DE VARIABLES	16
1.2.7 PALABRAS CLAVES.....	16
1.2.8 MARCO TEÓRICO	17
CAPÍTULO II: LEVANTAMIENTO DE INFORMACIÓN Y ESPECIFICACIÓN REQUERIMIENTOS ADA.....	21
2.1 LEVANTAMIENTO DE INFORMACIÓN	22
2.2 DEFINICIÓN DE REQUERIMIENTOS.....	25
2.3 ESPECIFICACIÓN DE REQUERIMIENTOS	27
2.4 DISEÑO DE pruebas	32
3 CAPÍTULO III: METODOLOGÍA	34
3.1 IMPLEMENTACIÓN API ADA	34
3.2 PASO A PASO DE UN REQUERIMIENTO	37
4 CAPÍTULO IV: METODOLOGÍA DE PRUEBAS.....	40
4.1 EVALUACIÓN ADA.....	40
4.1.2 DISEÑO DE PRUEBAS FUNCIONALES.....	41
4.1.3 EJECUCIÓN DE LAS PRUEBAS FUNCIONALES	42
5 DEFINICIÓN Y APLICACIÓN DEL CASO DE ESTUDIO	43

6	CONCLUSIONES Y RECOMENDACIONES.....	44
7	BIBLIOGRAFÍA	45
8	ANEXOS	46

Tabla 1 Plantilla Especificación de Requerimientos	27
Tabla 2 Ejemplo uso de Plantilla Especificación Caso de Uso Cambiar Estado Usuario	28
Tabla 3 Plantilla Especificación de Requerimientos: Agregar Usuario a Grupo	37
Tabla 4 Plantilla Casos de Prueba	41

Ilustración 1 Cuadro Comparativo Auth0 y Stormpath	23
Ilustración 2 Mockup Consulta Grupo	32
Ilustración 3 Mockup Crear Grupo.....	32
Ilustración 4 Mockup Crear Usuario	33
Ilustración 5 Fragmento Modelo Relacional	34
Ilustración 6 Servicios Rest	35
Ilustración 7 Diagrama Caso de Uso Agregar Usuario a Grupo	38
Ilustración 8 Fragmento Diagrama de Clases	39
Ilustración 9 Ejemplo Casos de PRueba	41
Ilustración 10 Fragmento Casos de Pruebas Diseñados: Agregar Usuario a Grupo	42
Ilustración 11 Informe de Pruebas Funcionales	42
Ilustración 12 Login Aplicación SAE	43

RESUMEN

Las compañías de software a la medida deben implementar una gran variedad de requerimientos que se repiten de una aplicación a otra. Por ejemplo, requerimientos no funcionales de AAA (Autenticación, Autorización y Auditoría) son implementados una y otra vez. En lugar de construir estos módulos de nuevo, las empresas podrían usar un módulo reutilizable que permita reducir los tiempos y costos de desarrollo.

Este proyecto se enfoca en la definición e implementación de *ADA* un API genérico que integre los requerimientos de AAA para la empresa *Software de Colombia*. Este sistema permite a los desarrolladores contar con un esquema de seguridad sin tener que implementarlo nuevamente. Los desarrolladores pueden definir las aplicaciones y sus opciones, y los administradores pueden definir grupos, usuarios, y permisos. El sistema provee opciones para restringir el acceso de los usuarios y generar rastros de auditoría.

Este documento describe el proceso llevado a cabo para definir e implementar el API, ilustra el proceso usando un caso de uso representativo y presenta una evaluación de la implementación. El documento presenta lo realizado en las actividades de (1) Levantamiento de Información, (2) Definición y Especificación de Requerimientos, (3) implementación de la Solución, (4) Pruebas y (5) Aplicación en un Caso de estudio.

INTRODUCCIÓN

La Seguridad es “la capacidad de un sistema para evitar acciones maliciosas o accidentales fuera del uso diseñado que afecta al sistema y evitar la divulgación o pérdida de información”¹

Un sistema seguro tiene por objeto proteger los activos y evitar el acceso no autorizado o modificación de información. Para implementar la seguridad, Sommerville ² propone tres requerimientos claves:

- * Autenticación, el proceso de identificación de los usuarios.
- * Autorización, especifican los privilegios y permisos de acceso de los usuarios identificados.
- * Auditoría: especifican como puede auditarse y comprobarse el uso del sistema.

Las empresas pueden implementar estos requerimientos usando sistemas comerciales como Auth01 y Stormpath, o soluciones opensource como Apache Shiro. Lamentablemente las soluciones comerciales implican costos adicionales de licenciamiento y operación, y las soluciones opensource no cuentan con interfaces visuales para la administración del sistema.

Este artículo presenta el proceso para el desarrollo de ADA, nuestra solución para implementar requerimientos no funcionales AAA en aplicaciones web.

El resto del artículo está organizado de la siguiente forma. La sección 2 presenta una introducción a los sistemas de AAA. La sección 3 describe la metodología usada para implementar los requerimientos AAA en ADA, nuestra API. La sección 4 ilustra la metodología usando el caso de uso Agregar Usuario a Grupo. La sección 5 describe el proceso de pruebas y evaluación. Y finalmente, la Sección 6, concluye el artículo.

¹ Microsoft. Microsoft [En línea] Fecha. 2016.[Citado 04-May-2016] Disponible en internet: <https://msdn.microsoft.com/en-us/library/ee658094.aspx>

² SOMERVILLE, Ian. Ingeniería del Software. Séptima Edición. Madrid. Pearson,2005, 182.

CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA

1. OBJETIVOS

1.1.1 Objetivo General

Implementar una solución genérica para requerimientos no funcionales de AAA (Autenticación, Autorización y Auditoría).

1.1.2 Objetivos Específicos:

- Diseñar una interfaz de programación (API) para los requerimientos de AAA.
- Construir un servicio o aplicación Web que implemente la API que permita identificar mejoras al desarrollo.
- Evaluar la solución usando un caso de estudio.

1.2 PROBLEMA

¿Cómo lograr la integración de requerimientos no funcionales de Autenticación, Autorización y Auditoría en una interfaz de programación de aplicaciones para software libre?

1.2.1 ANTECEDENTES

La empresa *Software de Colombia* se dedica a desarrollar sistemas de información a la medida que brinden soluciones efectivas e innovadoras a empresas aduaneras. En los 2 años de trabajo se ha visto involucrada en la construcción de aplicaciones para exportaciones y administración portuaria en las que debió construir módulos para la administración de usuarios, la definición de reglas de autorización y la generación de reportes de auditoría.

La construcción de estos módulos (usuarios, autorizaciones y auditoría) representó un costo muy alto para la empresa ya que requirió la implementación de un sistema bastante robusto por sus implicaciones en cuanto a seguridad y los posibles negativos efectos de un error en estos módulos en el negocio.

Para suplir los requerimientos mencionados, *Software de Colombia* no quería usar software propietario como *Ath0*³ o *Stormpath*⁴ para proteger su propiedad intelectual, no depender de otros proveedores y no incurrir en costos de licenciamientos adicionales.

Para las empresas que contratan los servicios de *Software de Colombia* son muy importantes requerimientos no funcionales de Autenticación, Autorización y Auditoría ya que manejan información sensible de otras empresas nacionales e internacionales, y el mal uso de esta información podría incurrir en algún delito. Por este motivo, las aplicaciones deben identificar a cada usuario, especificar los privilegios y permisos que tiene cada uno y hacer un seguimiento riguroso a cada una de las acciones que realizan.

Tanto en *Software de Colombia*, como en otras empresas, la implementación de los requerimientos AAA se ha hecho tradicionalmente usando:

- **Soluciones comerciales**, en donde se integra la base de datos y la interfaz de administración, pero las empresas deben incurrir en costos mensuales.
- O **Soluciones Opensource**, en donde no se tienen costos de licenciamiento, pero no suplen la totalidad de los requerimientos.

Por ejemplo, existen soluciones comerciales como *Auth0* y *Stormpath* que proveen servicios de autenticación y autorización:

- **Auth0:** permite implementar proveedores de identidad y personalizar la página de inicio de sesión de acceso, sin embargo, no cuenta con herramientas fuertes para el manejo de la auditoría.

³ Auth0 Inc. Auth0 [En línea] Fecha. 2015.[Citado 04-May-2016] Disponible en internet: <https://auth0.com/>

⁴ STORMPATH. Stormpath [En línea] Fecha. 2015.[Citado 04-May-2016] Disponible en internet: <https://stormpath.com/>

- **Stormpath:** permite implementar la autorización mediante roles y su autenticación permite el manejo y administración de tokens para el acceso a las aplicaciones, sin embargo, tiene una gran dependencia hacia los servicios de Apache Shiro.

Por otro lado, soluciones opensource como *Apache Shiro* no tienen una buena acogida por las empresas de desarrollo ya que, a pesar de prestar servicios como el de la auditoría a los usuarios, no cuenta con una interfaz gráfica para la administración de usuarios que permita interactuar fácilmente con ella.

En algunos casos, para suplir los requerimientos AAA es necesario combinar estas soluciones. Por ejemplo, es común combinar la solución de *Stormpath*, que cuenta con un sistema avanzado de administración de usuarios, grupos y roles con el sistema *Shiro*, que implementa los controles de seguridad en la aplicación.

Luego de analizar varias soluciones, la empresa *Software de Colombia* decidió construir un módulo que supla las necesidades y limitaciones de las soluciones existentes.

1.2.2 JUSTIFICACIÓN

A partir del análisis de las soluciones actuales (presentado en los antecedentes), este proyecto busca desarrollar una aplicación de software libre que cumpla con requerimientos no funcionales de Autenticación, Autorización y Auditoria para aplicaciones empresariales.

Esta solución será de gran utilidad para empresas como Software de Colombia que son empresas pequeñas o están surgiendo y no disponen de capital que les permita adquirir soluciones comerciales para disminuir la inversión de tiempos de desarrollo.

Adicionalmente, esta solución podrá ser de gran importancia para la universidad ya que permitirá contar con una aplicación de gran tamaño que podrá ser un caso de estudio o apoyo en las materias que implican construcción de software como Ingeniería de Software.

Finalmente, este proyecto es de gran importancia para los autores, ya que les permitirá llevar sus conocimientos de desarrollo a otras arquitecturas e implementación de herramientas no vistas durante su plan de estudios.

1.2.3 ALCANCES

El presente proyecto se centra en el diseño, desarrollo e implementación de un sistema reutilizable para la implementación de requerimientos no funcionales: Autenticación, Autorización y Auditoría.

1.2.4 LIMITES

El desarrollo de la aplicación se basará en los requerimientos definidos por la empresa *Software de Colombia*. Consideramos que estos requerimientos son aplicables a otras empresas del sector.

Igualmente, empresas con otros requerimientos podrán usar este software como base para la implementación de requerimientos no funcionales que ayudan a que las aplicaciones empresariales sean más seguras y completas.

De acuerdo al entorno de desarrollo de la empresa *Software de Colombia*, el software se desarrollará utilizando las siguientes herramientas y entornos de desarrollo:

- El lenguaje de programación Java,8.
- El servidor WildFly 10.0 que soporta las características de dicha plataforma.
- Servidor de bases de datos PostgreSQL

1.2.5 SISTEMAS DE HIPÓTESIS

Hipótesis de Trabajo: desarrollar una interfaz de programación que permita integrar de forma correcta los requerimientos AAA en una aplicación web

Hipótesis Nula: desarrollar una interfaz de programación no permitirá integrar de forma correcta los requerimientos AAA en una aplicación web

1.2.6 SISTEMAS DE VARIABLES

Variables Independientes:

- Requerimientos no funcionales AAA (Autenticación. Autorización y Auditoría)

Variables Dependientes:

- Aplicación WEB
- API

Variables Interviniente:

- Número de requerimientos deseados en la aplicación.
- Tiempo invertido en el desarrollo de requerimientos no funcionales.

1.2.7 PALABRAS CLAVES

- ✓ Requerimientos no funcionales.
- ✓ Autenticación.
- ✓ Autorización.
- ✓ Auditoría.

1.2.8 MARCO TEÓRICO

La seguridad es “la capacidad de un sistema para evitar acciones maliciosas o accidentales fuera del uso diseñado que afecta al sistema y evitar la divulgación o pérdida de información”⁵. Un sistema seguro tiene por objeto proteger los activos y evitar el acceso no autorizado o modificación de información. Existen tres principales áreas a las que se han dirigido los requerimientos de seguridad: Gobierno y aplicaciones militares; banca y finanzas; y aplicaciones científicas y académicas.

Para las aplicaciones gubernamentales y militares, la divulgación de información fue el principal riesgo que debía ser evitado a toda costa, para lograr esto las aplicaciones y los sistemas operativos eran desarrollados para hacer frente a la separación de los datos y procesos a través de hardware y software. En la banca y finanzas el énfasis está en la seguridad de la protección de los activos, mientras que la divulgación es un riesgo importante, el riesgo es mucho mayor al autorizar la modificación de la información, la protección de la integridad de la información produce la confianza de los clientes y por lo tanto la confianza en la institución responsable de mantener estos datos y procesos y para la computación científica y académica, el énfasis principal es la seguridad en la protección contra el uso de recursos no autorizados, esto se observa en la época en que los ordenadores y el tiempo de cálculo eran muy caros y los recursos eran críticos para la investigación y las aplicaciones científicas. Este énfasis ha llevado a las normas que existen en la administración del sistema y en la detección de intrusos.

No existe una estrategia de implementación única que se encuentre generalmente aceptada para aplicar todos factores de seguridad en un sistema, pero se han generalizado ciertos requerimientos que buscan desarrollar el proceso de seguridad; Ian Somerville en su libro Ingeniería del software⁶ agrupa estos requerimientos: AAA (Autenticación, Autorización y Auditoría) como parte de los requerimientos de protección definiéndolos así:

- Autenticación: es el proceso de identificación de los usuarios.
- Autorización: especifican los privilegios y permisos de acceso de los usuarios identificados.
- Auditoría: especifican como puede auditarse y comprobarse el uso del sistema.

Estos requerimientos se utilizan para evitar la suplantación de la identidad de los usuarios, poder Identificar que límites de acceso posee cada uno y además protege contra los daños al asegurar que se valide todas las entradas y

⁵ Microsoft. Microsoft [En línea] Fecha. 2016.[Citado 04-May-2016] Disponible en internet: <https://msdn.microsoft.com/en-us/library/ee658094.aspx>

⁶ SOMERVILLE, Ian. Ingeniería del Software. Séptima Edición. Madrid. Pearson,2005, 182.

salidas que se muestran cuando un usuario intenta manipular los datos, en adición también brinda un seguimiento de las actividades o acciones tomadas internamente dentro del sistema.

Este proceso no es fácil ya que para implementar los requerimientos de protección primero se deben identificar las deficiencias de seguridad o los aspectos del sistema que contribuyen a la generación de una falla, para ello es ideal abordar los procesos de análisis y síntesis que hacen parte del desarrollo del sistema, es decir: Identificar las condiciones o estados del sistema que pueden conducir a un accidente o eventos no planificados con consecuencias indeseables. Len Bass⁷ nos propone un escenario para documentar e identificar los requerimientos usando escenarios de atributos de calidad en el pretende identificar todos los posibles actores que conforman el sistema y que pueden afectarlo, esta implementación no solo distingue escenarios de atributos de calidad generales los cuales intentan definir sistemas independientes y pueden potencialmente pertenecer a cualquier sistema de atributo de calidad, también permiten generar atributos de calidad específicos para un sistema en particular en el marco de consideración del proyecto actual. A continuación, se explican los seis pasos para su realización:

1. Identificar la fuente de estímulo, esta es alguna entidad (un ser humano, un sistema u ordenador, o cualquier otro actor) que genera alguna alteración en el sistema.
2. Identificar el estímulo, es decir que condición se debe tener en cuenta cuando se ingresa a un sistema.
3. Identificar el medio ambiente, el estímulo se produce dentro de ciertas condiciones o entornos, ya sea que el sistema se encuentre en una condición de sobrecarga o puede estar en ejecución cuando se produce el estímulo.
4. Identificar el Artefacto, algunas partes del sistema mediante algunas acciones se pueden estimular.
5. Identificar la respuesta, es la actividad llevada a cabo después de la llegada del estímulo.
6. Medición de la respuesta, cuando se produce una respuesta en el sistema, dicha respuesta debe ser medible de alguna manera ya que con esto se busca que el requerimiento se puede probar.

Actualmente ya se tienen gobiernos como el de Estados Unidos⁸ que ha definido la AAA como un patrón de diseño que debe ser implementado en sus soluciones, este patrón busca realizar una autenticación correcta aumentando la seguridad y

⁷ BASS, Len. Arquitectura de software en práctica. [En línea] Fecha. 2016.[Citado 04-May-2016] Disponible en internet:

http://www.win.tue.nl/~wstomv/edu/2ii45/year-0910/Software_Architecture_in_Practice_2nd_Edition_Chapter4.pdf

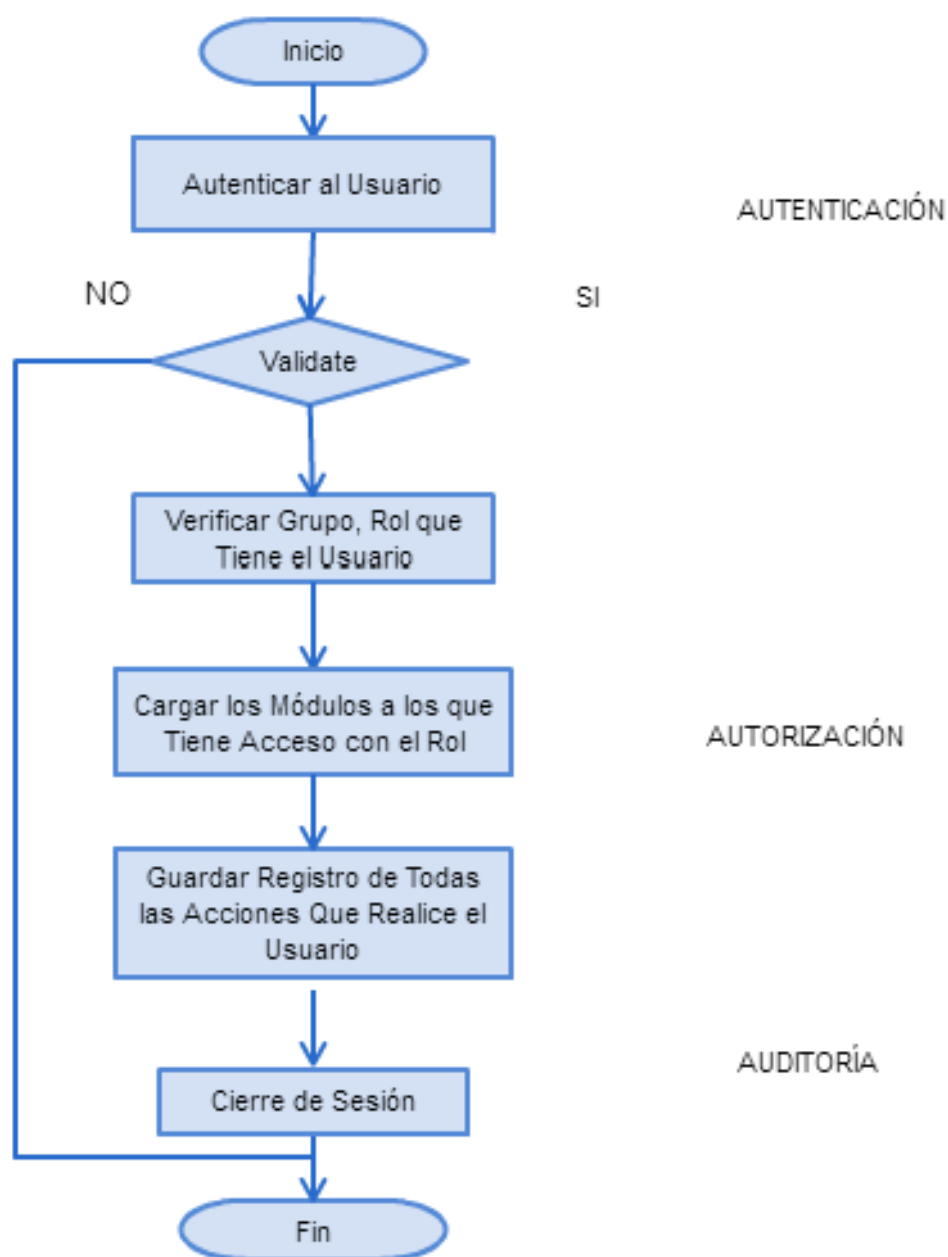
⁸ Paiva, Joe; Tibbis, Pau. Authentication, Authorization, and Audit Design Pattern: Internal User Identity Authentication Version 1.1. [En línea] Fecha. 2016.[Citado 04-May-2016] Disponible en internet: http://www.techstrategies.oit.va.gov/docs/designpatterns/AAADP_Inc1IntUserAuth04232014.pdf

disminuyendo el costo total de propiedad, las personas deben utilizar procedimientos de autenticación de identidad aprobados que verifiquen y tengan en cuenta la importancia y la sensibilidad de la información en un sistema, reconocer las amenazas y vulnerabilidades en el sistema.

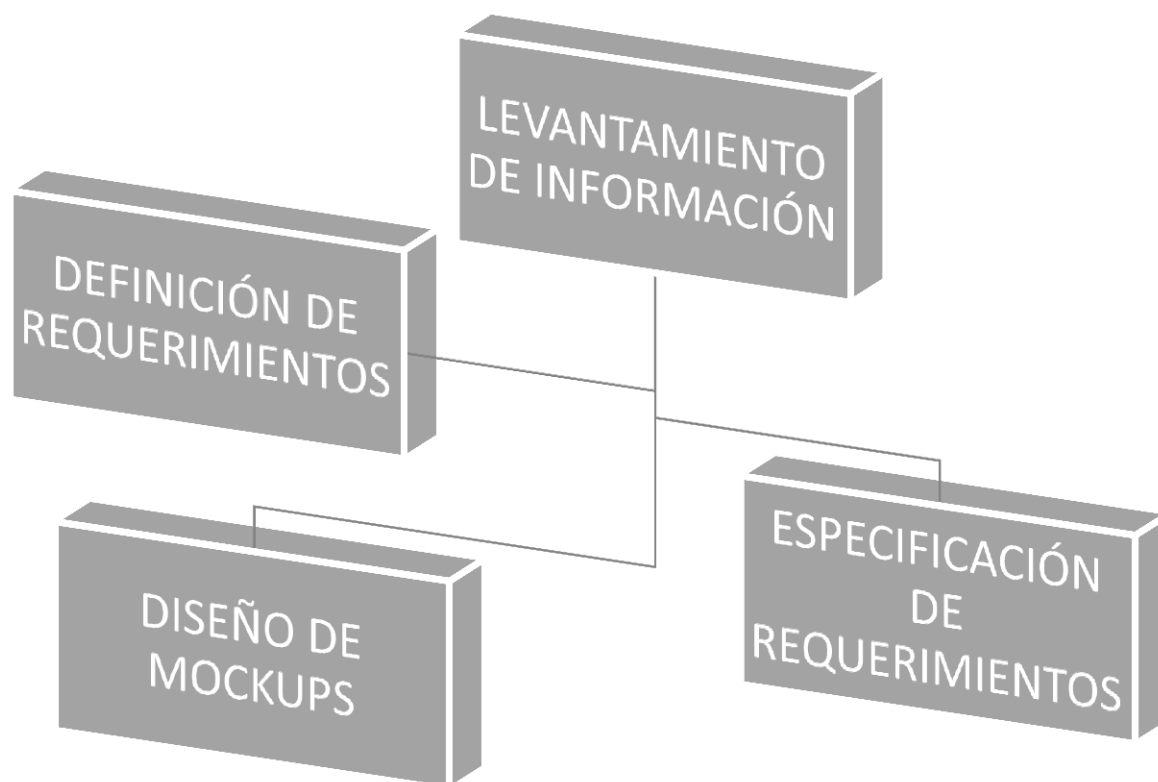
En la Universidad Interamericana para el Desarrollo ya se había propuesto por uno de sus estudiantes la integración de los de los requerimientos no funcionales AAA en los sistemas de información basándose en los roles.⁹

En dicho estudio exponen la pérdida de información y los costos en los que se puede incurrir al tener un software poco seguro y plantea como solución a esto la utilización los requerimientos AAA de donde se extrae el siguiente flujo en donde se evidencia la forma en la que se debe aplicar el protocolo sobre una aplicación.

⁹ ALARCON, David. Servivios de Autenticación, Autorización y Auditoría en los Sistemas de Información Utilizando un Enfoque Basado en Roles. [En línea] Fecha. 2016.[Citado 04-May-2016] Disponible en internet: https://prezi.com/ho_bhismehx/servicios-de-autenticacion-autorizacion-y-auditoria-en-los/



CAPÍTULO II: LEVANTAMIENTO DE INFORMACIÓN Y ESPECIFICACIÓN REQUERIMIENTOS ADA



2.1 LEVANTAMIENTO DE INFORMACIÓN

Luego de definir el problema y nuestros objetivos comenzamos con el levantamiento de información, realizando una búsqueda de interfaces de programación que proporcionan soluciones parciales a la implementación de requerimientos funcionales de Autenticación, Autorización y Auditoría.

A continuación, se realiza un cuadro comparativo entre *Auth0* y *StormPath*, dos de las soluciones comerciales más utilizadas en este tipo de aplicaciones:

		AUTH0	STORMPATH
CREACIÓN DE APLICACIÓN		Permite ser integrado al desarrollo de una aplicación.	Permite ser integrado al desarrollo de una aplicación.
	FRONTEND	Permite la utilización de: Vanilla JS, JQuery, Angular JS, SOCKET.IO y EmberJS	Permite la utilización de: JSON
	BACKEND	Permite la utilización de: asp.net web api, asp.net web api (own), node.js api, go, ruby api, ruby on rails api, php api, php (laravel) api, java api, spring security java api, python api, y .net wcf	Permite los siguientes lenguajes de programación: Java, Python, PHP y Ruby
	DATA BASE	Permite la utilización de: aws, azure mobile services, firebase, salesforce, salesforce(sandbox, sap odata)	Los datos pueden ser importados desde otro servicio, generados por la aplicación o introducidos por usuario.
MULTIPLATAFORMA		Permite el desarrollo multiplataforma.	-
MÚLTIPLES SDK		Permite la utilización de múltiples SDK.	No permite múltiples SDK solo el proporcionado por Stormpath.
INTEGRACIÓN BOX		Permite la integración con Box.	-
ADMINISTRACIÓN DE USUARIOS		Permite añadir, eliminar o bloquear usuarios. Permite modificar perfil Permite autorización de atributos Permite la identificación de la causa de origen del inicio de sesión de los usuarios.	Permite crear y guardar números de cuentas de usuario. Permite asignar usuarios a grupos. Permite implementar una API REST para administrar usuarios. Permite administrar a los usuarios en la consola de administración web.
INTERFAZ		Permite personalizar la interfaz con código HTML y java script.	Posee un plugin que trae pantallas básicas no personalizables.
AUTENTICACIÓN		Permite realizar la autenticación. Permite identificar los detalles de autenticación (historia de inicio de sesión y ubicaciones y dispositivos).	Permite realizar la autenticación. Incorpora RBAC para el manejo de permisos basados en roles.
PERFILES		Permite crear perfiles detallados para cada uno de sus usuarios	Permite crear un perfil de usuario estándar. Permite adaptar los perfiles de usuarios con datos personalizados. Permite la utilización de perfiles de usuario para un sistema SaaS.
GRUPO		-	Permite realizar configuraciones de permisos a nivel de grupo. Permite realizar agrupación organizativas como equipo o función.

CONEXIONES	SOCIAL	Facebook, Twitter, etc..	Facebook, Twitter, etc..
	EMPRESA	Permite la utilización de: AD, LDAP, SAML	Permite la utilización de: AD, LDAP(Microsoft Active Directory, Open LDAP, Apache DS, Solaris LDAP, Novell eDirectory, y RedHat DS), y cuentas con un Directorio Stormpath en la nube.
	BASE DE DATOS	Permite la creación de forma segura de base de datos de Auth0 o en la proporcionada por el usuario.	Permite conexiones con bases de datos
	SIN CONTRASEÑA	Permite la utilización de conexiones que no requieren que el usuario recuerde una contraseña	No permite la utilización de la aplicación sin contraseña.
EXTENSIBILIDAD	REGLAS	Permite la configuración de reglas que se ejecutan como parte del proceso de autenticación cada vez que un usuarios ingresan a una aplicación.	No permite la configuración de reglas
	CORREOS ELECTRONICOS	Permite personalizar las plantillas de correo electrónico para verificación de los usuarios, Genera correos que permite el cambio de contraseñas y dar la bienvenida a la aplicación.	Permite el envío de correos configurables a los nuevos usuarios después de registrarse Permite reestablecer la contraseña, las contraseñas no se envían a través de correo electrónico. Permite la personalización de los correos electrónicos con su propio código HTML de marca.
	COMPLEMENTOS	-	No permite la utilización de complementos.
MOBILE		Permite trabajar con las plataformas (IOS, Android y Windows Phone 8). Permite la autenticación a través del widget de mobile-ready.	-
SEGURIDAD		-	Permite la publicación de los datos a través de HTTPS Stormpath. Permite la utilización de TLS (SSL) cifrado. Permite generar y gestionar Claves API y tokens OAuth.
ENTIDADES		Users, Context, Console, Rules, Protocol, Profile, Endpoints, Client, Grants	Account, Directory, Group, Account, Collection Resource Application
OPERACIONES		GET, POST , addRolesToUser, callback, push, UnauthorizedError, access_token, userinfo, state, connectionStrategy, lifetimeInSeconds, request, refresh_token, read, update, delete, signup, signupCallback, v2PatchUser, audience, recipient, createUpnClaim, passthroughClaimsWithNoMapping, mapUnknownClaimsAsIs, mapIdentities, signResponse	href, accountStore, listIndex, isDefaultAccountStore, isDefaultGroupStore, createdAt, modifiedAt, GET, POST, moreInfo, developerMessage, offset, limit, size, items, directories, tenant, passwordResetTokens, loginAttempts, accountStoreMapping, defaultAccountStoreMapping, defaultGrupoStoreMapping, verificationEmailStatus, verificationSuccessEmailStatus, welcomeEmailStatus, resetSuccessEmailStatus, resetTokenTtl, maxLength, minLength, minLowerCase, minNumeric, minUpperCase,
AUDITORIA		Se hace una integración con Auth0 y Loggly mediante varias configuraciones realizadas utilizando webtask	Se hace una integración utilizando Shiro o utilizando framework como Audit4j

Ilustración 1 Cuadro Comparativo Auth0 y Stormpath

Auth0: simplifica la autenticación de los usuarios en las aplicaciones ya que crearon una arquitectura de identificación y autorización genérica que puede ser empleada en cualquier negocio que involucre la administración y gestión de usuarios.

Sin embargo, Auth0 no cumple con nuestro tercer requerimiento la Auditoría ya que no cuenta con una herramienta integrada para realizar la tarea de seguimiento de actividades a los usuarios.

Stormpath: no solo maneja una arquitectura de identificación de usuarios si no que adicionalmente permite el manejo de jerarquías permitiendo la creación de grupos roles y permisos de forma fácil y ahorrando muchas líneas de código ya que utiliza Servicios REST para ello.

Sin embargo, la interfaz gráfica que tiene no es personalizable y tampoco cumple con las condiciones de nuestro tercer requerimiento de auditoría.

Luego de revisar las características y soluciones ofrecidas por estas APIs para la implementación de las AAA en conjunto con la empresa Software de Colombia realizamos la definición de los requerimientos que nos ayudarían a darle solución a la problemática presentada en los antecedentes.

2.2 DEFINICIÓN DE REQUERIMIENTOS

1. **ADMINISTRACIÓN:** Módulo encargado de la configuración de los servicios relacionados con la seguridad de la aplicación; es decir con la creación de grupos, roles, permisos que se le pueden asignar a los usuarios que tengan acceso a la aplicación y que cuenten con diferentes perfiles:
 - Crear Usuario.
 - Consultar Usuario.
 - Actualizar Usuario.
 - Cambiar Estado Usuario.
 - Crear Grupo.
 - Consultar Grupo.
 - Actualizar Grupo.
 - Crear Rol.
 - Consultar Roles.
 - Actualizar Roles.
 - Crear Permiso.
 - Consultar Permiso.
 - Actualizar Permiso.
 - Agregar Rol a Grupo.
 - Agregar Usuario a Grupo
 - Agregar Rol a Usuario.
 - Crear Tipo de Recurso.
 - Consultar Tipo de Recurso.
 - Actualizar tipo de Recurso.
 - Consultar Acción.

2. **USUARIO (Self Service):** Módulo en el que se encuentran los servicios que pueden realizar los usuarios sobre sus propias cuentas, administración y configuración de su perfil de usuario:

- Inicio de Sesión Básico.
- Inicio de Sesión con Redes Sociales.
- Inicio de Sesión con Token.
- Inicio de Sesión Captcha.
- Modificar Password.
- Actualizar Datos.
- Actualizar Imagen de Perfil.
- Cerrar Sesión.

3. **Aplicación:** Módulo encargado de configurar los servicios que va a realizar la aplicación a los que podrá acceder el usuario según el grupo al que pertenezca y sus roles asignados:

- Crear Reportes.
- Consultar Reportes.
- Actualizar Reportes
- Crear Aplicación.
- Consultar Aplicación.
- Actualizar Aplicación.
- Registro Log Eventos

2.3 ESPECIFICACIÓN DE REQUERIMIENTOS

Para la especificación de los requerimientos se realizó la creación de una plantilla para diligenciar toda la información pertinente a cada requerimiento:

- ✓ Id del requerimiento
- ✓ Nombre
- ✓ Categoría
- ✓ Actores
- ✓ Casos de Usos Asociados
- ✓ Propósito
- ✓ Datos de Entrada
- ✓ Datos de Salida
- ✓ Precondiciones
- ✓ Restricciones
- ✓ Controles
- ✓ Flujo Normal de Trabajo
- ✓ Flujo Alternativo

Tabla 1 Plantilla Especificación de Requerimientos

IDENTIFICADOR CASO DE USO:		NOMBRE:	
CATEGORÍA:			
ACTORES:			
CASOS DE USO ASOCIADOS:			
PROPÓSITO:			
DATOS DE ENTRADA:			
Id.	Nombre	Tipo de Dato	Validaciones
1			
DATOS DE SALIDA:			
Id.	Nombre	Tipo de Dato	Validaciones
1			
PRECONDICIONES:			
•			
RESTRICCIONES:			
•			

IDENTIFICADOR CASO DE USO:		NOMBRE:
CONTROLES:		
•		
FLUJO NORMAL DE TRABAJO 1:		
Paso	Actor	Sistema
1		
2		
3		
4		
5		
FLUJO Alterno:		
Paso	Actor	Sistema
1		
2		
3		
4		
5		

A continuación, la plantilla diligenciada con el requerimiento *Cambiar Estado a un Usuario*:

Tabla 2 Ejemplo uso de Plantilla Especificación Caso de Uso Cambiar Estado Usuario

IDENTIFICADOR CASO DE USO: ADM_03		NOMBRE: Cambiar Estado a un Usuario	
CATEGORÍA: Administración			
ACTORES: Usuario Administrador, Sistema			
CASOS DE USO ASOCIADOS:			
<ul style="list-style-type: none"> • Actualizar Usuario. • Consultar Usuario. 			
PROPÓSITO:			
<ul style="list-style-type: none"> • Permitir al usuario administrador activar o desactivar un usuario. 			
DATOS DE ENTRADA:			
Id.	Nombre	Tipo de Dato	Validaciones
1	Usuario	String	Usuario Existente
2	Nombres Usuario	String	
3	Apellidos	String	
4	Estado	String	
DATOS DE SALIDA:			
Id.	Nombre	Tipo de Dato	Validaciones

IDENTIFICADOR CASO DE USO: ADM_03			NOMBRE: Cambiar Estado a un Usuario
1	Imagen de Perfil	JPG	Información no editable
2	Nombres Usuario	String	Información no editable
3	Apellidos	String	Información no editable
4	Contraseña	String	Información no editable
5	Confirmación Contraseña	String	Información no editable
6	Género	String	Información no editable
7	Dirección	String	Información no editable
8	Número Celular	INT	Información no editable
6	País	String	Información no editable
10	Estado/Departamento	String	Información no editable
11	Ciudad	String	Información no editable
12	Código Postal	INT	Información no editable
13	Captcha	String	Información no editable
14	Aceptación de los términos y condiciones del aplicativo.	Boolean	Información no editable
PRECONDICIONES: <ul style="list-style-type: none"> • Usuario Administrador debe estar registrado en la aplicación. • Usuario a cambiar estado debe estar registrado en la aplicación 			
RESTRICCIONES: <ul style="list-style-type: none"> • Usuario no tiene permisos para hacer la consulta • Usuario no tiene permisos para cambio de estado 			
CONTROLES: <ul style="list-style-type: none"> • 			
FLUJO NORMAL DE TRABAJO 1 Cambiar Estado Usuario Activo:			
Paso	Actor	Sistema	
1	Usuario Administrador ingresa a la aplicación		
2		Se solicita Logging	
3	Se autentica el Usuario Administrador		
4		Valida los permisos que tiene el usuario y carga la aplicación con el perfil	
5	Ingresa a la opción de Consulta Usuario		
6		Se despliega el formulario de Consulta	
7	Ingresa los parámetros para realizar la consulta del usuario Activo		
8		El sistema verifica que el usuario a consultar existe	

IDENTIFICADOR CASO DE USO: ADM_03		NOMBRE: Cambiar Estado a un Usuario
9		El sistema trae la información del usuario.
10	Usuario Administrador selecciona estado inactivo.	
11	Usuario administrador guarda el cambio	
12		Solicita confirmación del cambio.
13	Usuario Administrador confirma el cambio	
14		Guarda el cambio de estado.
FLUJO NORMAL DE TRABAJO 2 Cambiar Estado Usuario In Activo:		
Paso	Actor	Sistema
1	Usuario Administrador ingresa a la aplicación	
2		Se solicita Logging
3	Se autentica el Usuario Administrador	
4		Valida los permisos que tiene el usuario y carga la aplicación con el perfil
5	Ingresa a la opción de Consulta Usuario	
6		Se despliega el formulario de Consulta
7	Ingresa los parámetros para realizar la consulta del usuario Inactivo	
8		El sistema verifica que el usuario a consultar existe
9		El sistema trae la información del usuario.
10	Usuario Administrador selecciona estado activo.	
11	Usuario administrador guarda el cambio	
12		Solicita confirmación del cambio.
13	Usuario Administrador confirma el cambio	
14		Guarda el cambio de estado.
FLUJO Alterno DE TRABAJO 1 Consulta Usuario No Existe:		
Paso	Actor	Sistema
1	Usuario Administrador ingresa a la aplicación	
2		Se solicita Logging

IDENTIFICADOR CASO DE USO: ADM_03		NOMBRE: Cambiar Estado a un Usuario
3	Se autentica el Usuario Administrador	
4		Valida los permisos que tiene el usuario y carga la aplicación con el perfil
5	Ingresa a la opción de Consulta	
6		Se despliega el formulario de Consulta
7	Ingresa los parámetros para realizar la consulta de un usuario inexistente.	
8		El sistema verifica que el usuario a consultar no existe
9		Devuelve mensaje con el resultado de la consulta indicando que el usuario no existe.

Nota: Para ver la especificación completa diríjase a la sección de Anexos (Anexo 1 Especificación de Requerimientos; Identificador Caso de Uso ADM_03 Página: 77)

2.4 DISEÑO DE MOCKUPS

Para la creación de los *mockups* y poder avanzar en el desarrollo del cliente web, se utilizó el *framework primefaces* y archivos web *xhtml*.

Consulta Grupo

Nombre del grupo	
------------------	--

ConsultarNuevo

Resultado Consulta Grupo		
Nombre del Grupo	Descripción	Estado

Ilustración 2 Mockup Consulta Grupo

Crear Grupo

Nombre del Grupo *		Descripción: *	
--------------------	--	----------------	--

Usuarios

Roles

CrearCancelar

Ilustración 3 Mockup Crear Grupo

Crear Usuario

Usuario: *	<input type="text"/>	Nombre: *	<input type="text"/>
Apellido: *	<input type="text"/>	Correo Electronico: *	<input type="text"/>
Confirmacion Correo Electronico: *	<input type="text"/>	Numero Celular:	<input type="text"/>
Direccion:	<input type="text"/>	Contraseña: *	<input type="text"/>
Confirmar Contraseña: *	<input type="text"/>	Pais:	<input type="text"/>
Ciudad:	<input type="text"/>	Codigo Postal:	<input type="text"/>

Ilustración 4 Mockup Crear Usuario

Nota: Para ver en su totalidad los *mockups* diríjase a la sección de Anexos.
Página 113

3 CAPÍTULO III: METODOLOGÍA

3.1 IMPLEMENTACIÓN API ADA

Para el desarrollo del software ADA, se realizaron los siguientes pasos para asegurar a cabalidad que este cumpla los objetivos planteados.

Se empezó con el levantamiento del modelo relacional de acuerdo con lo especificado en el SRS y en los *Mockups*. Este implementa un modelo de RBAC (*Role-based access control*), el cual es una alternativa al modelo de seguridad de todo o nada de los sistemas tradicionales basados en superusuario. En este se puede dar a los usuarios la capacidad de resolver sus propios problemas mediante la asignación de paquetes de privilegios adecuados, que tienen capacidades que suelen ser otorgadas a un superusuario. Se pueden dividir dichas capacidades en varios paquetes y asignarlas por separado a individuos que comparten las responsabilidades administrativas.

El modelo relacional creado consta de diferentes secciones:

1. La sección de usuario: Que tiene al usuario y a los parámetros de seguridad de este.
2. La sección de permisos: Que está constituido por los roles, grupos y acciones.
3. La sección de auditoria: Que consta de todas las tablas generadas por el @auditory - envers de JEE.
4. La sección de la aplicación: Es la sección que va relacionada directamente con la aplicación, donde se encuentran las aplicaciones registradas, las imágenes y los recursos.

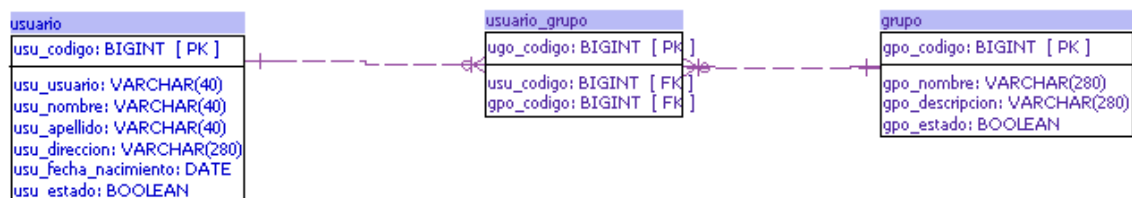


Ilustración 5 Fragmento Modelo Relacional

Teniendo como base el modelo relacional se realizan los scripts, que serán ejecutados en el motor de base de datos PostgreSQL.

- I. Se realizaron los diagramas de clases correspondientes a la parte del back-end de la aplicación, lo que incluye la sección de persistencia y del negocio de la aplicación.

- II. Se hizo el mapeo de las entidades con el método revange utilizando Hibernate y se crearon los DAOs correspondientes. Creando a su vez los DTOs para el transporte de la información.
- III. Se crean las excepciones para el adecuado manejo de errores, como la creación y configuración del log de errores.
- IV. Se establece un modelo de seguridad utilizando Apache Shiro¹⁰ el cual es un marco de gran alcance y fácil de utilizar la seguridad de Java que realiza la autenticación, la autorización, la criptografía, y la gestión de sesiones. Para esto se crea el archivo shito.ini y se realiza su correspondiente configuración.
- V. Se realizan los servicios RESTFul, ya que son más livianos que los servicios SOAP y nos permiten una mayor rapidez, la cual es esencial ya que estos pueden ser consumidos desde una aplicación móvil o desde una aplicación responsive. Para poder implementarlos en una aplicación cliente, se realiza el api de dichos servicios.

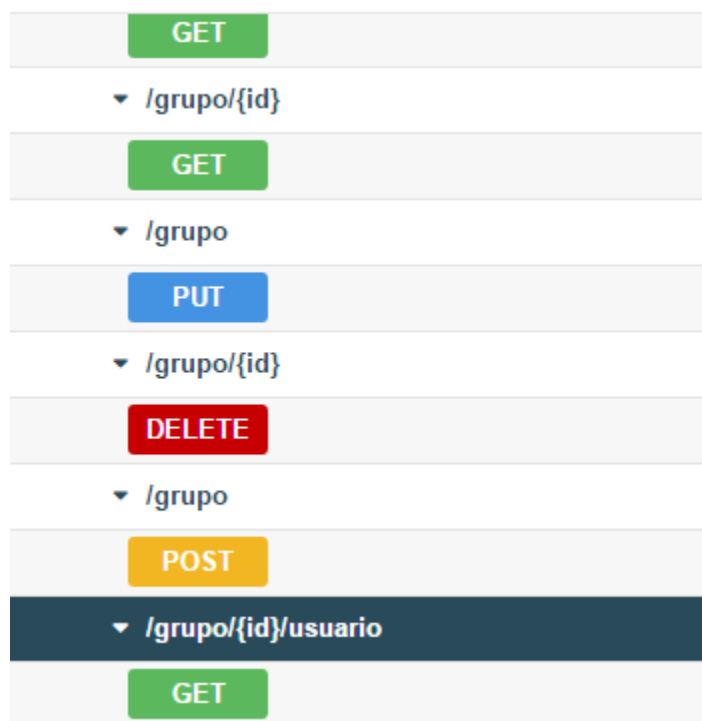


Ilustración 6 Servicios Rest

- VI. Se realiza la aplicación web cliente que pueda consumir los servicios ya mencionados. Esta se elabora con el framework primefaces, JavaScript,

¹⁰ The Apache Software Foundation. Apache Shiro. [En línea] Fecha. 2015.[Citado 04-May-2016] Disponible en internet: <http://shiro.apache.org/>

servlets, y la herramienta de para la gestión de herramientas de gestión de proyectos de software y comprensión MAVEN.

3.2 PASO A PASO DE UN REQUERIMIENTO

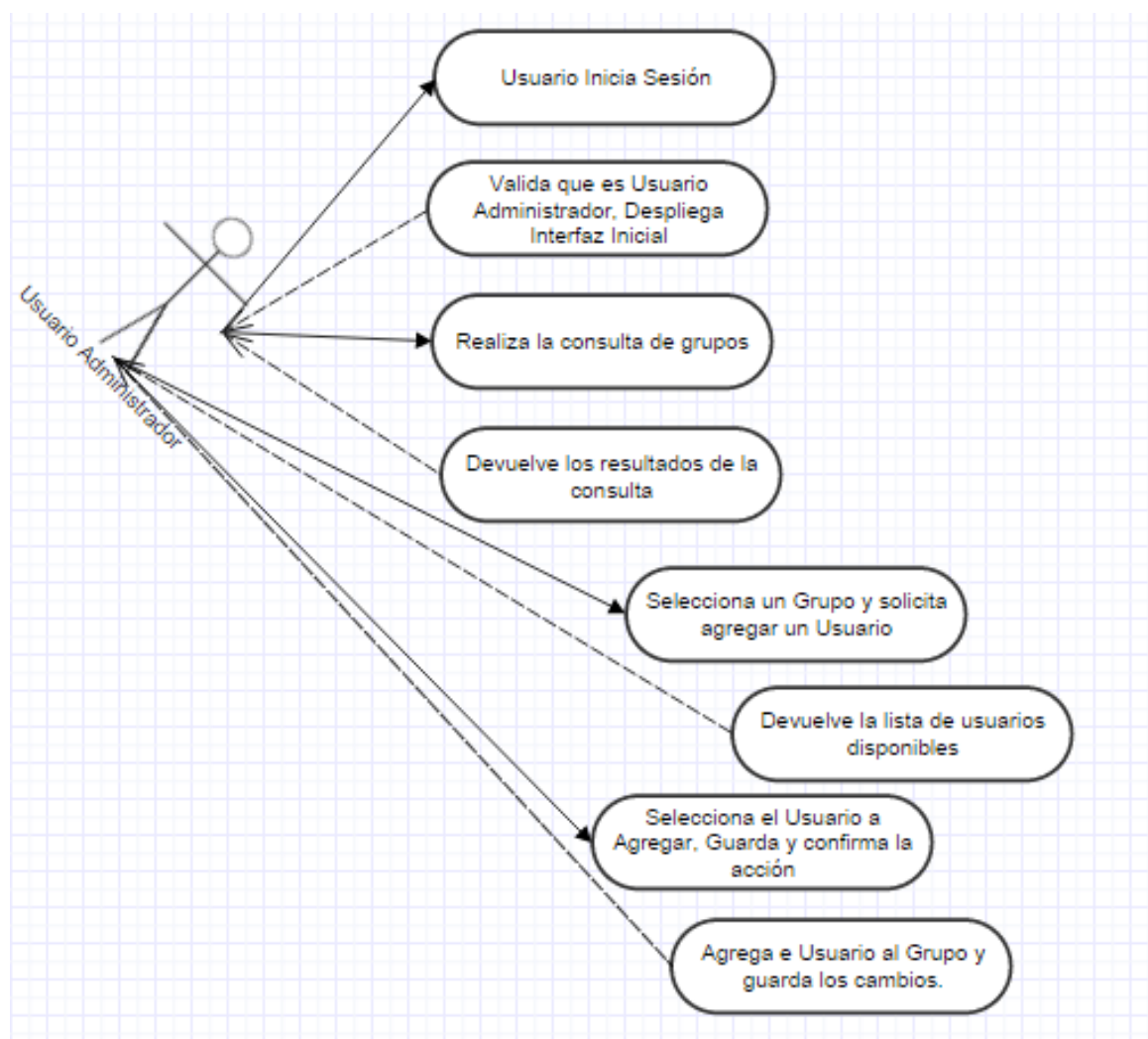
Se escogió el caso de uso: Asociar Usuario a un Grupo para mostrar el paso a paso de la implementación.

ESPECIFICACIÓN:

Tabla 3 Plantilla Especificación de Requerimientos: Agregar Usuario a Grupo

IDENTIFICADOR CASO DE USO: ADM_18		NOMBRE: Agregar Usuario a Grupo	
CATEGORÍA: Administración			
ACTORES: Usuario Administrador, Sistema			
CASOS DE USO ASOCIADOS: <ul style="list-style-type: none">No Aplica			
PROPÓSITO: <ul style="list-style-type: none">Permitir al usuario administrador agregar Usuario a un grupo.			
DATOS DE ENTRADA:			
Id.	Nombre	Tipo de Dato	Validaciones
1	Nombre del Usuario	String	String mayor a 1 carácter
DATOS DE SALIDA:			
Id.	Nombre	Tipo de Dato	Validaciones
1			
PRECONDICIONES: <ul style="list-style-type: none">Usuario administrador debe estar registrado en la aplicación.Usuario administrador debe tener permisos para agregar Usuario a Grupo			
RESTRICCIONES: <ul style="list-style-type: none">No Aplica			
CONTROLES: <ul style="list-style-type: none">EL Usuario a agregar al grupo no debe estar agregado previamente.El Usuario a agregar al grupo debe tener un rol asignado.			
FLUJO NORMAL DE TRABAJO 1: Agregar Usuario a Grupo			
Paso	Actor	Sistema	
1	Usuario Administrador accede a la opción de Actualizar Grupo.		
2	Da clic en el botón de Agregar Usuario		
3		Carga la lista de Usuarios existentes en la aplicación.	

IDENTIFICADOR CASO DE USO: ADM_18		NOMBRE: Agregar Usuario a Grupo
4	Selecciona los Usuarios que desea agregar al grupo.	
5	Da clic en el botón agregar Usuarios	
		Guarda el cambio realizado

DIAGRAMA CASO DE USO:*Ilustración 7 Diagrama Caso de Uso Agregar Usuario a Grupo***DIAGRAMA DE CLASES:****IMPLEMENTACIÓN:**

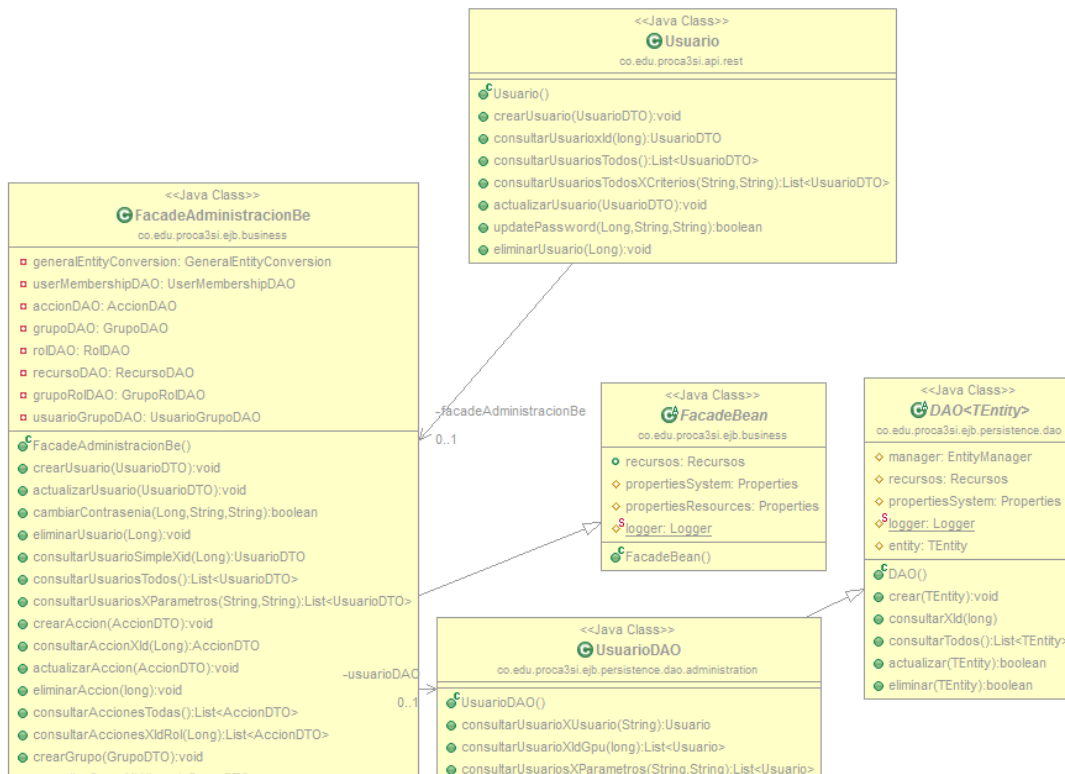
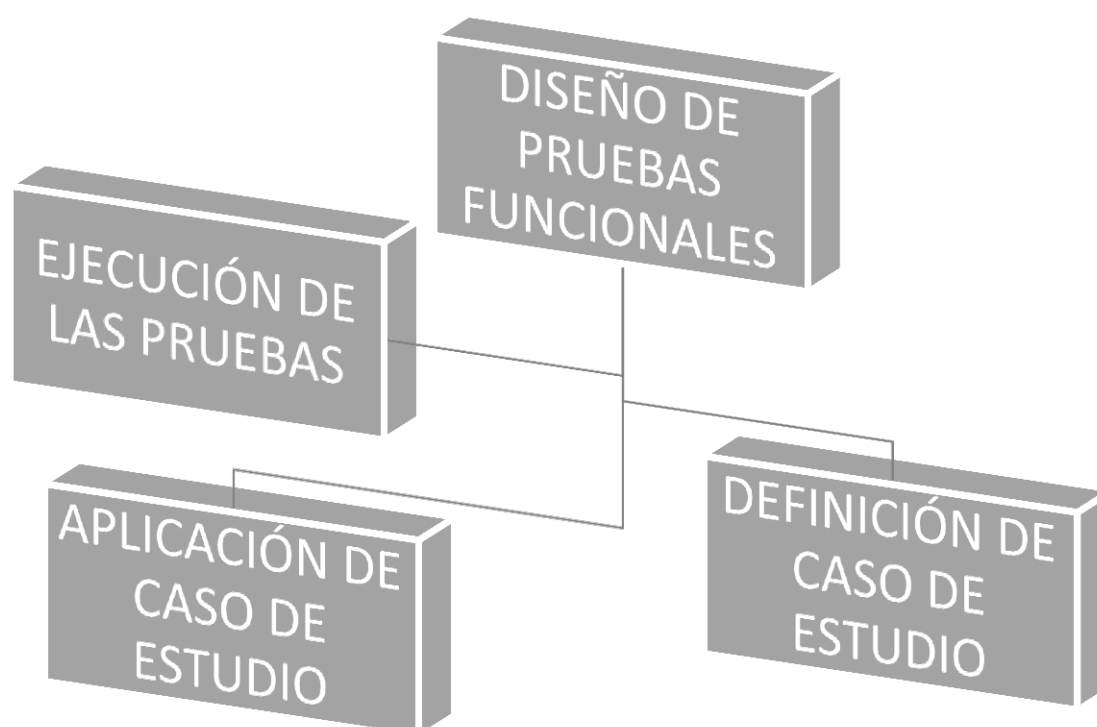


Ilustración 8 Fragmento Diagrama de Clases

4 CAPÍTULO IV: METODOLOGÍA DE PRUEBAS

4.1 EVALUACIÓN ADA



4.1.2 DISEÑO DE PRUEBAS FUNCIONALES

Las pruebas funcionales son las pruebas que se le aplican a cada una de las funcionalidades o partes de una aplicación para certificar que se encuentra funcionando de acuerdo a la definición y especificación de cada uno de los requerimientos.

Para el diseño de las pruebas se creó la siguiente plantilla:

Tabla 4 Plantilla Casos de Prueba

Id escenario	Escenario	Id caso de prueba	Caso de prueba	Resultado esperado	Resultado Final
1		1.1			
		1.2			
		1.3			
2		2.1			
		2.2			
		2.3			

Por metodología definida con la empresa Software de Colombia se decide en la plantilla únicamente colocar los casos, el resultado esperado y el final ya el paso a paso se podría ver en las ejecuciones y toma de evidencias de cada uno de ellos.

Estos son algunos de los casos de prueba que se diseñaron:

Id escenario	Escenario	Id caso de prueba	Caso de prueba	Resultado esperado	Resultado Final
1	Inicio Sesión Básico	1.1	Ingresar usuario que este registrado con contraseña correcta	Acceso a la aplicación	
		1.2	Ingresar usuario que este registrado con contraseña incorrecta	No permite ingreso a la aplicación, solicita ingresar de nuevo datos.	
		1.3	Ingresar usuario que no se encuentre registrado con contraseña correcta	No permite ingreso a la aplicación, solicita ingresar de nuevo datos.	
		1.4	Ingresar usuario que este registrado pero que no se encuentre activo	No permite ingreso a la aplicación y aparece mensaje de error	
		1.5	Ingreso erroneo de contraseña por tres ocasiones seguidas	Se bloquea usuario, debe solicitar reseteo de contraseña	
2	Inicio de Sesión con Redes Sociales		Ingresar usuario que este registrado y campo contraseña en blanco	Muestra mensaje de error solicitando contraseña valida aplicación	
		2.1	Seleccionar a red social registrada	No permite ingreso y se debe seleccionar red social o registrarse en la aplicación	
3	Modificar Password	2.2	Seleccionar a red social no registrada		
		3.1	Ingresar contraseña actual, nueva y confirmación valida	Contraseña modificada exitosamente	
		3.2	Ingresar contraseña actual, nueva valida, confirmación distinta	Muestra mensaje de error en campo confirmacion contraseña se debe volver a digitar	
		3.3	Ingresar contraseña actual invalida, nueva valida, confirmacion valida	Muestra mensaje de error en campo contraseña actual	
		3.4	Ingresar contraseña actual, nueva y confirmación iguales pero no cumple características	Muestra mensaje de error, se debe volver a ingresar contraseña con características validas	
		3.5	Ingresar contraseña actual, nueva y confirmación no ingresar nada	Muestra mensaje de error en donde debe agregar contraseña con datos validos	

Ilustración 9 Ejemplo Casos de Prueba

4.1.3 EJECUCIÓN DE LAS PRUEBAS FUNCIONALES

25	Agregar Usuario a Grupo				
		25.1	Agregar como administrador un usuario a un grupo existente en la aplicación	La aplicación permite agregar a un usuario a un grupo	Exitoso
		25.2	Agregar como administrador un usuario a un grupo no existente en la aplicación	La aplicación arroja un mensaje de error y solicita ingresar un grupo que exista en la aplicación	Exitoso

Ilustración 10 Fragmento Casos de Pruebas Diseñados: Agregar Usuario a Grupo

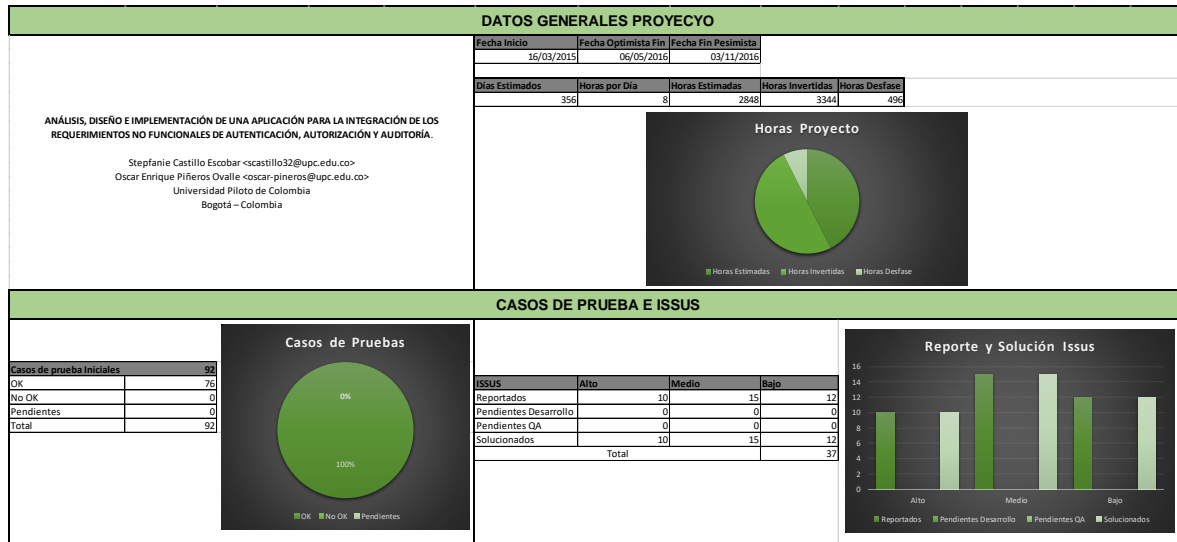


Ilustración 11 Informe de Pruebas Funcionales

5 DEFINICIÓN Y APLICACIÓN DEL CASO DE ESTUDIO

Para evaluar la aplicabilidad de la solución se definió el siguiente caso de estudio:

Se realizó la implementación en un software previamente creado en la materia Ingeniería de Software denominado “SAE” donde se implementaron los servicios del software ADA. Y se utiliza la interfaz de ADA, para poder utilizar y administrar los reportes de auditoria.



The screenshot displays the SAE application interface. At the top, there is a green header bar with the text "SAE" on the left. To the right of the header, there are two input fields labeled "Correo Electronico *" and "Contraseña *", followed by a blue button labeled "Entrar a SAE". Below the header, the main content area is divided into two sections. On the left, there is a large image of a green 3D figure holding a key to unlock a large padlock. On the right, there is a "Registry" form with the following fields: "First Name *", "Last Name *", "Date of Birth *", "Sex-select *" (with radio buttons for "female", "male", and "other"), "e-mail *", "Phone:", "Phone with Ext:", "Password 1: *", and "Password 2: *". Below the form fields are two buttons: "Reset" and "Save". At the bottom of the page, there is a footer bar with several links: "Terminos y condiciones", "Sobre Nosotros", "Contacto", "Condiciones generales de contartacion SAE", and "Sobre Cars".

Ilustración 12 Login Aplicación SAE

6 CONCLUSIONES Y RECOMENDACIONES

Nuestra investigación en torno a los requerimientos AAA nos permitió entender que las aplicaciones que se construyen en la actualidad deben ser lo más seguras posibles. Algunas organizaciones, como por ejemplo entidades del estado, incluyen estos tres requerimientos como condiciones mínimas en sus aplicaciones.

En la actualidad existen varias soluciones comerciales y *opensource* que permiten implementar los requerimientos de AAA. En muchos casos, es necesario combinar estas soluciones para lograr satisfacer los requerimientos más exigentes en temas de seguridad.

Como parte de este proyecto se construyó un sistema reutilizable para el manejo de seguridad y la implementación de requerimientos de AAA. Para el desarrollo se combinaron *frameworks opensource* para la implementación de esquemas de seguridad, como Apache Shiro, así como otras librerías estándar en Java como JPA y JAX-RS.

La solución se diseñó e implementando REST con el fin de facilitar su reuso en diferentes tipos de aplicaciones. Por ejemplo, puede ser usado en aplicaciones Java y *Javascript*. Igualmente, se incluyó el uso de JWT para mantener esquemas de seguridad entre clientes web y la aplicación. Curiosamente, el desarrollo de estas APIs REST resulta bastante fácil a través de las librerías estándar de JAX-RS.

El desarrollo tuvo varios problemas en su implementación, como lo fueron la configuración de seguridad a través del shiro.ini, que en su última versión no permite la implementación del SALT, elemento utilizado para la encriptación de la clave. Como también la implementación y creación de reportes con iReport y la implementación de listas generadas con los reportes de Envers.

7 BIBLIOGRAFÍA

- Auth0 Inc. Auth0 [En línea] Fecha. 2015.[Citado 04-May-2016] Disponible en internet: <https://auth0.com/>
- STORMPATH. Stormpath [En línea] Fecha. 2015.[Citado 04-May-2016] Disponible en internet: <https://stormpath.com/>
- Chapter 16: Quality Attributes. Microsoft [En línea] Fecha. 2016.[Citado 04-May-2016] Disponible en internet: <https://msdn.microsoft.com/en-us/library/ee658094.aspx>
- SOMERVILLE, Ian. Ingeniería del Software. Séptima Edición. Madrid. Pearson, 2005, P 182.
- BASS, Len. Arquitectura de software en práctica. [En línea] Fecha. 2016.[Citado 04-May-2016] Disponible en internet: http://www.win.tue.nl/~wstomv/edu/2ii45/year0910/Software_Architecture_in_Practice_2nd_Edition_Chapter4.pdf
- Paiva, Joe; Tibbis, Pau. Authentication, Authorization, and Audit Design Pattern: Internal User Identity Authentication Version 1.1. [En línea] Fecha. 2016.[Citado 04-May-2016] Disponible en internet: http://www.techstrategies.oit.va.gov/docs/designpatterns/AAADP_Inc1IntUserAuth04232014.pdf
- ALARCON, David. Servicios de Autenticación, Autorización y Auditoría en los Sistemas de Información Utilizando un Enfoque Basado en Roles. [En línea] Fecha. 2016.[Citado 04-May-2016] Disponible en internet: https://prezi.com/ho_bhisgmehx/servicios-de-autenticacion-autorizacion-y-auditoria-en-los/
- The Apache Software Foundation. Apache Shiro. [En línea] Fecha. 2015.[Citado 04-May-2016] Disponible en internet: <http://shiro.apache.org/>
- Sznajdleder, Pablo. JEE 7 a Fondo Diseño y desarrollo de aplicaciones Java Enterprise. Primera Edición. MARCOMBO, S.A., 2015, PP 260.

8 ANEXOS

1. Especificación De Requerimientos

MÓDULO USUARIO (Self Service) ADA

IDENTIFICADOR CASO DE USO: USU_01		NOMBRE: Inicio Sesión Básico	
CATEGORÍA: Usuario			
ACTORES: Usuario, Sistema			
CASOS DE USO ASOCIADOS: <ul style="list-style-type: none">Reestablecer contraseña			
PROPÓSITO: <ul style="list-style-type: none">Permitir al usuario ingresar a la aplicación con su información personal Usuario y Contraseña.Permitir al sistema identificar quien ingresa a la aplicación y que configuración determinada debe cargar.			
DATOS DE ENTRADA:			
Id.	Nombre	Tipo de Dato	Validaciones
1	Usuario	String	Usuario Válido
2	Contraseña	String	Contraseña válida para el usuario ingresado
DATOS DE SALIDA:			
Id.	Nombre	Tipo de Dato	Validaciones
1			
2			
3			
PRECONDICIONES: <ul style="list-style-type: none">Usuario debe estar registrado en la aplicación.Usuario debe estar activo.			
RESTRICCIONES: <ul style="list-style-type: none">Usuario se encuentra bloqueado.Contraseña inválidaSupera el número de intentos permitidos para ingresar			
CONTROLES: <ul style="list-style-type: none">Longitud de usuarioLongitud y características de contraseñaEstado del usuario			
FLUJO NORMAL DE TRABAJO 1 Ingreso con Contraseña:			
Paso	Actor	Sistema	
1	Usuario ingresa a la aplicación.		
2		Carga el Login de la Aplicación	
3	Ingresa Usuario y Contraseña		
4		Valida si la información es correcta	
5		Despliega la aplicación con la configuración del usuario.	
FLUJO Alterno 1 Error en Contraseña:			
Paso	Actor	Sistema	

IDENTIFICADOR CASO DE USO: USU_01		NOMBRE: Inicio Sesión Básico
1	Usuario ingresa a la aplicación.	
2		Carga el Login de la Aplicación
3	Ingresa Usuario y Contraseña errada	
4		Valida que la información de la contraseña es errada
5		Solicita al usuario ingresar nuevamente los datos
6	Usuario ingresa nuevamente los datos	

IDENTIFICADOR CASO DE USO: USU_02		NOMBRE: Inicio de Sesión con Redes Sociales	
CATEGORÍA: Usuario			
ACTORES: Usuario, Sistema			
CASOS DE USO ASOCIADOS: <ul style="list-style-type: none">Reestablecer contraseña			
PROPÓSITO: <ul style="list-style-type: none">Permitir al usuario ingresar a la aplicación con información registrada en alguna red social.Permitir al sistema identificar quien ingresa a la aplicación y que configuración determinada debe cargar.			
DATOS DE ENTRADA:			
Id.	Nombre	Tipo de Dato	Validaciones
1	Red Social	Botón	Redirige a la red social seleccionada
2	Usuario	String	Usuario Válido
3	Contraseña	String	Contraseña válida para el usuario ingresado
DATOS DE SALIDA:			
Id.	Nombre	Tipo de Dato	Validaciones
1			
2			
3			
PRECONDICIONES: <ul style="list-style-type: none">Usuario debe tener una cuenta en la red social seleccionada.Usuario debe estar registrado en la aplicación.Usuario debe estar activo.			
RESTRICCIONES: <ul style="list-style-type: none">Usuario se encuentra bloqueado.Sesión en la red social no activa.			
CONTROLES: <ul style="list-style-type: none">Longitud de usuarioLongitud y características de contraseñaEstado del usuario			
FLUJO NORMAL DE TRABAJO 1 Ingreso Red Social:			
Paso	Actor	Sistema	
1	Usuario ingresa a la aplicación.		
2		Carga el Login de la Aplicación	
3	Usuario selecciona red social		
4		Carga el acceso a la red social y valida la sesión.	
5	Acepta el ingreso con la red social		
6		Valida si la información es correcta	

IDENTIFICADOR CASO DE USO: USU_02		NOMBRE: Inicio de Sesión con Redes Sociales
7		Despliega la aplicación con la configuración del usuario.
FLUJO Alterno 1 Sesión de Red Social no Activa:		
Paso	Actor	Sistema
1	Usuario ingresa a la aplicación.	
2		Carga el Login de la Aplicación
3	Usuario selecciona red social	
4		Carga el acceso a la red social sesión no iniciada
5	Ingresa Usuario y Contraseña de la red social	
6		Valida que la información de la red social es correcta
7		Despliega la aplicación con la configuración del usuario.

IDENTIFICADOR CASO DE USO: USU_03		NOMBRE: Inicio de Sesión Captcha	
CATEGORÍA: Usuario			
ACTORES: Usuario, Sistema			
CASOS DE USO ASOCIADOS: <ul style="list-style-type: none">Reestablecer contraseña			
PROPÓSITO: <ul style="list-style-type: none">Permitir al usuario ingresar a la aplicación con verificación de código captchaPermitir al sistema identificar quien ingresa a la aplicación y que configuración determinada debe cargar.			
DATOS DE ENTRADA:			
Id.	Nombre	Tipo de Dato	Validaciones
1	Usuario	String	Usuario Válido
2	Contraseña	String	Contraseña válida para el usuario ingresado
3	Factor de Verificación Captcha	String	Código ingresado igual mostrado al usuario
DATOS DE SALIDA:			
Id.	Nombre	Tipo de Dato	Validaciones
1			
2			
3			
PRECONDICIONES: <ul style="list-style-type: none">Usuario debe estar registrado en la aplicación.Usuario debe estar activo.Usuario debe tener configurado el inicio de sesión con código captcha.			
RESTRICCIONES: <ul style="list-style-type: none">Usuario se encuentra bloqueado.Sesión en la red social no activa.Código Captcha incorrecto			
CONTROLES: <ul style="list-style-type: none">Longitud de usuarioLongitud y características de contraseñaEstado del usuario			
FLUJO NORMAL DE TRABAJO 1 Ingreso con Código Captcha:			
Paso	Actor	Sistema	
1	Usuario ingresa a la aplicación.		
2		Carga el Login de la Aplicación	
3	Ingresa Usuario y Contraseña		
4		Valida si la información es correcta	
5		Solicita ingresar código Captcha	

IDENTIFICADOR CASO DE USO: USU_03		NOMBRE: Inicio de Sesión Captcha
6	Usuario ingresa Código Captcha	
7		Valida que el código ingresado corresponda al mostrado al usuario.
FLUJO Alterno 1 Sesión código Captcha Errado:		
Paso	Actor	Sistema
1	Usuario ingresa a la aplicación.	
2		Carga el Login de la Aplicación
3	Ingresa Usuario y Contraseña	
4		Valida si la información es correcta
5		Solicita ingresar código Captcha
6	Usuario ingresa Código Captcha de forma errada	
7		Valida que el código ingresado es errado
8		Solicita volver a ingresar el código
9	EL usuario ingresa nuevamente el código Captcha	

IDENTIFICADOR CASO DE USO: USU_04			NOMBRE: Inicio de Sesión con Token
CATEGORÍA: Usuario			
ACTORES: Usuario, Sistema			
CASOS DE USO ASOCIADOS: <ul style="list-style-type: none">Reestablecer contraseña			
PROPÓSITO: <ul style="list-style-type: none">Permitir al usuario ingresar a la aplicación con verificación de TokenPermitir al sistema identificar quien ingresa a la aplicación y que configuración determinada debe cargar.			
DATOS DE ENTRADA:			
Id.	Nombre	Tipo de Dato	Validaciones
1	Usuario	String	Usuario Válido
2	Contraseña	String	Contraseña válida para el usuario ingresado
3	Factor de Verificación Token	String	Token igual al enviado al usuario
DATOS DE SALIDA:			
Id.	Nombre	Tipo de Dato	Validaciones
1			
2			
3			
PRECONDICIONES: <ul style="list-style-type: none">Usuario debe estar registrado en la aplicación.Usuario debe estar activo.Usuario debe tener configurado el inicio de sesión Token.			
RESTRICCIONES: <ul style="list-style-type: none">Usuario se encuentra bloqueado.Sesión en la red social no activa.Token incorrecto			
CONTROLES: <ul style="list-style-type: none">Longitud de usuarioLongitud y características de contraseñaEstado del usuario			
FLUJO NORMAL DE TRABAJO 1 Ingreso con Código Captcha:			
Paso	Actor	Sistema	
1	Usuario ingresa a la aplicación.		
2		Carga el Login de la Aplicación	
3	Ingresa Usuario y Contraseña		
4		Valida si la información es correcta	
5		Solicita ingresar Clave de Token	
6	Usuario ingresa Clave Token		

IDENTIFICADOR CASO DE USO: USU_04		NOMBRE: Inicio de Sesión con Token
7		Valida que la clave ingresada por el usuario corresponde a la indicada en el Token.
		Despliega la aplicación con la configuración del usuario.
FLUJO Alternativo 1 Sesión con Token Errado:		
Paso	Actor	Sistema
1	Usuario ingresa a la aplicación.	
2		Carga el Login de la Aplicación
3	Ingresa Usuario y Contraseña	
4		Valida si la información es correcta
5		Solicita ingresar Clave de Token
6	Usuario ingresa Clave Token errada	
7		Valida que la clave ingresada por el usuario es errada
8		Solicita el ingreso nuevamente de la clave del Token
9	EL usuario ingresa nuevamente la clave de Token	

IDENTIFICADOR CASO DE USO: USU_05		NOMBRE: Modificar Password	
CATEGORÍA: Usuario			
ACTORES: Usuario, Sistema			
CASOS DE USO ASOCIADOS: <ul style="list-style-type: none">Reestablecer contraseña			
PROPÓSITO: <ul style="list-style-type: none">Modificar la contraseña del usuario desde el perfil del mismo.			
DATOS DE ENTRADA:			
Id.	Nombre	Tipo de Dato	Validaciones
1	Contraseña Actual	Sring	Contraseña válida para el usuario
2	Contraseña Nueva	String	Contraseña cumple con las características establecidas.
3	Confirmación de la Contraseña	String	Contraseña debe coincidir con la ingresada en el campo contraseña nueva.
DATOS DE SALIDA:			
Id.	Nombre	Tipo de Dato	Validaciones
1			
2			
3			
PRECONDICIONES: <ul style="list-style-type: none">Usuario debe estar registrado en la aplicación.Usuario debe estar activo.Usuario debe estar en sesión			
RESTRICCIONES: <ul style="list-style-type: none">Usuario se encuentra bloqueado.Contraseña inválida			
CONTROLES: <ul style="list-style-type: none">Longitud y características de contraseñaEstado del usuario			
FLUJO NORMAL DE TRABAJO 1 Ingreso con Contraseña:			
Paso	Actor	Sistema	
1	Usuario inicia sesión.		
2		Carga la sesión del usuario con los permisos asociados al usuario.	
3	Usuario ingresa a Modificar Contraseña		
4		Carga el formulario de modificación de contraseña	
5	Usuario ingresa contraseña actual		
6		Valida que la contraseña ingresada sea	

IDENTIFICADOR CASO DE USO: USU_05		NOMBRE: Modificar Password
		correcta
7	Usuario ingresa la nueva contraseña	
8		Sistema valida que la contraseña ingresada cumpla con las características definidas.
9	Usuario ingresa la confirmación de la contraseña.	
10		Valida que la contraseña ingresada coincida con la que se digitó en el campo nueva contraseña.
11	Usuario guarda el cambio realizado	
FLUJO Alterno 1 Contraseña Actual Errada:		
Paso	Actor	Sistema
1	Usuario inicia sesión.	
2		Carga la sesión del usuario con los permisos asociados al usuario.
3	Usuario ingresa a Modificar Contraseña	
4		Carga el formulario de modificación de contraseña
5	Usuario ingresa contraseña actual diferente.	
6		Valida que la contraseña ingresada no es correcta
10		Solicita rectificar la contraseña.
11	Usuario ingresa de forma correcta la contraseña actual	
12		Valida que la contraseña ingresada es correcta
13	Usuario ingresa la nueva contraseña	
14		Sistema valida que la contraseña ingresada cumpla con las características definidas.
15	Usuario ingresa la confirmación de la contraseña.	
16		Valida que la contraseña ingresada coincida con la que se digitó en el campo nueva contraseña.
17	Usuario guarda el cambio realizado	
FLUJO Alterno 2 Contraseña Nueva no Cumple con Características:		
Paso	Actor	Sistema
1	Usuario inicia sesión.	
2		Carga la sesión del usuario con los permisos asociados al usuario.

IDENTIFICADOR CASO DE USO: USU_05		NOMBRE: Modificar Password
3	Usuario ingresa a Modificar Contraseña	
4		Carga el formulario de modificación de contraseña
5	Usuario ingresa contraseña actual	
6		Valida que la contraseña ingresada sea correcta
10	Usuario ingresa la nueva contraseña sin las características establecidas	
11		Sistema valida que la contraseña ingresada no cumple con las características definidas.
12		Solicita que ingrese nuevamente una contraseña que cumpla con las características correctas.
13	Usuario ingresa nuevamente la contraseña nueva con las características correctas	
14		Sistema valida que la contraseña ingresada cumple con las características definidas.
15	Usuario ingresa la confirmación de la contraseña.	
16		Valida que la contraseña ingresada coincida con la que se digitó en el campo nueva contraseña.
17	Usuario guarda el cambio realizado	
FLUJO Alternativo 3 Confirmación de la Contraseña Errada:		
Paso	Actor	Sistema
1	Usuario inicia sesión.	
2		Carga la sesión del usuario con los permisos asociados al usuario.
3	Usuario ingresa a Modificar Contraseña	
4		Carga el formulario de modificación de contraseña
5	Usuario ingresa contraseña actual	
6		Valida que la contraseña ingresada sea correcta
10	Usuario ingresa la nueva contraseña.	
11		Sistema valida que la contraseña ingresada cumple con las características definidas.
12	Usuario ingresa la confirmación de la contraseña diferente a la nueva	

IDENTIFICADOR CASO DE USO: USU_05		NOMBRE: Modificar Password
	contraseña.	
13		Valida que la contraseña ingresada no coincide con la que se digitó en el campo nueva contraseña.
14		Solicita ingresar nuevamente la confirmación de la clave.
15	Usuario ingresa la confirmación de la contraseña de forma correcta	
16		Valida que la contraseña ingresada coincida con la que se digitó en el campo nueva contraseña.
17	Usuario guarda el cambio realizado	

IDENTIFICADOR CASO DE USO: USU_06		NOMBRE: Actualizar Datos	
CATEGORÍA: Usuario			
ACTORES: Usuario Administrador, Sistema			
CASOS DE USO ASOCIADOS: <ul style="list-style-type: none">• Modificar Password.• Actualizar Imagen de Perfil			
PROPÓSITO: <ul style="list-style-type: none">• Permite que el usuario actualice su información.			
DATOS DE ENTRADA:			
Id.	Nombre	Tipo de Dato	Validaciones
1	Imagen de Perfil	JPG	Imagen correcta
2	Nombres Usuario	String	Longitud, Requerido
3	Apellidos	String	Longitud, Requerido
4	Contraseña	String	Características correctas
5	Confirmación Contraseña	String	Contraseña igual a la anterior
6	Género	String	Una sola Opción
7	Dirección	String	
8	Número Celular	INT	
6	País	String	
10	Estado/Departamento	String	
11	Ciudad	String	
12	Código Postal	INT	Requerido USA
13	Captcha	String	
14	Aceptación de los términos y condiciones del aplicativo.	Boolean	
DATOS DE SALIDA:			
Id.	Nombre	Tipo de Dato	Validaciones
1			
2			
3			
PRECONDICIONES: <ul style="list-style-type: none">• Usuario debe estar registrado en la aplicación.			
RESTRICCIONES: <ul style="list-style-type: none">• Usuario no tiene permisos para hacer la actualización de su información			
CONTROLES: <ul style="list-style-type: none">• Usuario ingresado ya existe.• Campos requeridos para guardar el formulario• Si el usuario ingresa contraseña que cumpla con las características.			
FLUJO NORMAL DE TRABAJO 1 Actualización de Usuario:			
Paso	Actor	Sistema	
1	Usuario ingresa a la aplicación		

IDENTIFICADOR CASO DE USO: USU_06		NOMBRE: Actualizar Datos
2		Se solicita Logging
3	Se autentica el Usuario	
4	Ingresa a la opción de Actualizar Datos	
5		Se despliega el formulario de Actualización
6	Usuario actualiza la información que requiere	
7	Se aceptan términos y condiciones	
8		El sistema verifica que los campos requeridos de formulario estén diligenciados
9		Solicita confirmación de la actualización
10	Usuario confirma la actualización	
11		Guarda los cambios realizados en la información
12	Usuario cierra la sesión.	

IDENTIFICADOR CASO DE USO: USU_07		NOMBRE: Actualizar Imagen de Perfil	
CATEGORÍA: Usuario			
ACTORES: Usuario, Sistema			
CASOS DE USO ASOCIADOS: <ul style="list-style-type: none">Actualizar DatosActualizar Password			
PROPÓSITO: <ul style="list-style-type: none">Permitir al usuario salir de la aplicación una vez terminada su labor			
DATOS DE ENTRADA:			
Id.	Nombre	Tipo de Dato	Validaciones
1	Imagen Perfil	JPG	
DATOS DE SALIDA:			
Id.	Nombre	Tipo de Dato	Validaciones
1			
2			
3			
PRECONDICIONES: <ul style="list-style-type: none">El usuario debe estar en sesión en la aplicaciónEl usuario debe tener permiso para actualizar su información.			
RESTRICCIONES: <ul style="list-style-type: none">Sesión Expirada.El usuario no tiene permisos.			
CONTROLES:			
FLUJO NORMAL DE TRABAJO 1 Actualizar Imagen de Perfil:			
Paso	Actor	Sistema	
1	Usuario inicia sesión en la aplicación		
2		Valida a que grupo y roles pertenece el usuario.	
3		Carga la sesión del usuario	
4	Usuario ingresa al menú modificar imagen.		
5		Carga el formulario de actualizar imagen.	
6	Usuario ingresa al catálogo de imágenes.		
7		Carga el catálogo de imágenes	
8	Usuario selecciona una imagen del catálogo		
9	Usuario guarda el cambio		
10		Solicita confirmación del cambio	
11	Usuario confirma el cambio		

IDENTIFICADOR CASO DE USO: USU_07		NOMBRE: Actualizar Imagen de Perfil
12		Guarda el cambio del usuario y despliega la ventana inicio.
FLUJO Alternativo DE TRABAJO 1 Cierre Sesión Expirada:		
Paso	Actor	Sistema
1	Usuario da clic en el botón, Link de cierre de Sesión	
2		Verifica que el usuario no se encuentra en sesión
3		Indica que no existe sesión
4		Despliega el Login de la aplicación
5	El usuario cierra la aplicación	

IDENTIFICADOR CASO DE USO: USU_08		NOMBRE: Cerrar sesión usuario	
CATEGORÍA: Usuario			
ACTORES: Usuario, Sistema			
CASOS DE USO ASOCIADOS: <ul style="list-style-type: none">			
PROPÓSITO: <ul style="list-style-type: none">Permitir al usuario salir de la aplicación una vez terminada su labor			
DATOS DE ENTRADA:			
Id.	Nombre	Tipo de Dato	Validaciones
1			
2			
3			
4			
DATOS DE SALIDA:			
Id.	Nombre	Tipo de Dato	Validaciones
1			
2			
3			
PRECONDICIONES: <ul style="list-style-type: none">El usuario debe estar en sesión en la aplicación			
RESTRICCIONES: <ul style="list-style-type: none">Sesión Expirada			
CONTROLES:			
FLUJO NORMAL DE TRABAJO 1 Cierre Sesión:			
Paso	Actor	Sistema	
1	Usuario da clic en el botón, Link de cierre de Sesión		
2		Verifica que el usuario se encuentra en sesión	
3		Solicita confirmación del cierre de Sesión	
4	Usuario confirma el cierre de Sesión		
5		Se cierra la aplicación	
FLUJO Alterno DE TRABAJO 1 Cierre Sesión Expirada:			
Paso	Actor	Sistema	
1	Usuario da clic en el botón, Link de cierre de Sesión		
2		Verifica que el usuario no se encuentra en sesión	
3		Indica que no existe sesión	
4		Despliega el Logging de la aplicación	

IDENTIFICADOR CASO DE USO: USU_08		NOMBRE: Cerrar sesión usuario
5	El usuario cierra la aplicación	

MÓDULO ADMINISTRACIÓN ADA

IDENTIFICADOR CASO DE USO: ADM_01		NOMBRE: Registrar Usuario	
CATEGORÍA: Administración			
ACTORES: Usuario Administrador, Sistema			
CASOS DE USO ASOCIADOS: <ul style="list-style-type: none">Inicio de Sesión (básico, Captcha, Token)Modificar Password.Actualizar Datos.Actualizar Imagen de Perfil.Cerrar Sesión.Asignar Grupo.Asignar Usuario al Rol.Actualizar Usuario.Consultar Usuario.			
PROPÓSITO: <ul style="list-style-type: none">Permitir al usuario administrador ingresar la información básica de un usuario y registrarlo en la aplicación			
DATOS DE ENTRADA:			
Id.	Nombre	Tipo de Dato	Validaciones
1	Imagen de Perfil	JPG	Imagen correcta
2	Usuario	String	Longitud, Usuario no Existente, Requerido
3	Nombres Usuario	String	Longitud, Requerido
4	Apellidos	String	Longitud, Requerido
5	Contraseña	String	Características correctas, Requerido
6	Confirmación Contraseña	String	Contraseña igual a la anterior, Requerido
7	Género	String	Una sola Opción, Requerido
8	Dirección	String	
9	Número Celular	INT	
10	e-Mail	String	Formato correcto, Requerido
11	País	String	Requerido
12	Estado/Departamento*	String	
13	Ciudad	String	
14	Código Postal	INT	Requerido USA
15	Captcha	String	
16	Aceptación de los términos y condiciones del aplicativo.	Boolean	Requerido
DATOS DE SALIDA:			
Id.	Nombre	Tipo de Dato	Validaciones
1			
2			

IDENTIFICADOR CASO DE USO: ADM_01		NOMBRE: Registrar Usuario	
3			
PRECONDICIONES:			
<ul style="list-style-type: none"> • Usuario no debe estar registrado en la aplicación. 			
RESTRICCIONES:			
<ul style="list-style-type: none"> • Usuario ya se encuentra registrado • Contraseña no cumple con las características • Usuario debe ser único 			
CONTROLES:			
<ul style="list-style-type: none"> • Usuario ingresado ya existe. • Campos requeridos para guardar el formulario • Si el usuario ingresa contraseña que cumpla con las características. 			
FLUJO NORMAL DE TRABAJO 1 Registro de Usuario:			
Paso	Actor	Sistema	
1	Usuario Administrador ingresa a la aplicación		
2		Se solicita Logging	
3	Se autentica el Usuario Administrador		
4		Valida los permisos que tiene el usuario y carga la aplicación con el perfil	
5	Ingresa a la opción de registrar usuario		
6		Se despliega el formulario de registro	
7	Usuario selecciona la imagen de perfil		
8	Ingresa el ID Usuario		
9		Sistema verifica que el usuario ingresado no exista	
10	Se ingresa Nombres y Apellidos del usuario que se va a crear		
11	Se ingresa contraseña		
12		El sistema verifica que la contraseña cumpla con las características necesarias	
13	Se ingresa la confirmación de la contraseña		
14		El sistema verifica que la contraseña ingresada coincida con la ingresada anteriormente	
15	Se ingresan los demás datos básicos del usuario a crear		
16	Se aceptan términos y condiciones		

IDENTIFICADOR CASO DE USO: ADM_01		NOMBRE: Registrar Usuario
17		El sistema valida que se hallan ingresado todos los campos requeridos
18		El sistema guarda y crea el nuevo usuario
FLUJO Alterno DE TRABAJO 1 Usuario ya Existe:		
Paso	Actor	Sistema
1	Usuario Administrador ingresa a la aplicación	
2		Se solicita Logging
3	Se autentica el Usuario Administrador	
4		Valida los permisos que tiene el usuario y carga la aplicación con el perfil
5	Ingresa a la opción de registrar usuario	
6		Se despliega el formulario de registro
7	Usuario selecciona la imagen de perfil	
8	Ingresa el ID Usuario de uno existente	
9		Sistema verifica que el usuario ingresado existe
10		Solicita ingresar un nuevo ID Usuario
11	Usuario Administrador ingresa un nuevo ID Usuario	
12		Sistema verifica que el usuario ingresado no existe
13	Se ingresa Nombres y Apellidos del usuario que se va a crear	
14	Se ingresa contraseña	
15		El sistema verifica que la contraseña cumpla con las características necesarias
16	Se ingresa la confirmación de la contraseña	
17		El sistema verifica que la contraseña ingresada coincida con la ingresada anteriormente
18	Se ingresan los demás datos básicos del usuario a crear	
19	Se aceptan términos y condiciones	
20		El sistema valida que se hallan ingresado todos los campos requeridos
21		El sistema guarda y crea el nuevo usuario

IDENTIFICADOR CASO DE USO: ADM_02		NOMBRE: Consultar Usuario	
CATEGORÍA: Administración			
ACTORES: Usuario Administrador, Sistema			
CASOS DE USO ASOCIADOS: <ul style="list-style-type: none">Actualizar Usuario.Cambiar de estado.			
PROPÓSITO: <ul style="list-style-type: none">Permitir al usuario administrador consultar la información de un usuario y acceder a los menús de modificación de usuario(Actualizar Password, Cambiar de estado, Desbloquear usuario)			
DATOS DE ENTRADA:			
Id.	Nombre	Tipo de Dato	Validaciones
1	Usuario	String	Usuario Existente
2	Nombres Usuario	String	
3	Apellidos	String	
4	Estado	String	
DATOS DE SALIDA:			
Id.	Nombre	Tipo de Dato	Validaciones
1	Imagen de Perfil	JPG	Información no editable
2	Nombres Usuario	String	Información no editable
3	Apellidos	String	Información no editable
4	Contraseña	String	Información no editable
5	Confirmación Contraseña	String	Información no editable
6	Género	String	Información no editable
7	Dirección	String	Información no editable
8	Número Celular	INT	Información no editable
6	País	String	Información no editable
10	Estado/Departamento	String	Información no editable
11	Ciudad	String	Información no editable
12	Código Postal	INT	Información no editable
13	Captcha	String	Información no editable
14	Aceptación de los términos y condiciones del aplicativo.	Boolean	Información no editable
PRECONDICIONES: <ul style="list-style-type: none">Usuario debe estar registrado en la aplicación.			
RESTRICCIONES: <ul style="list-style-type: none">Usuario no tiene permisos para hacer la consulta			
CONTROLES: <ul style="list-style-type: none">			
FLUJO NORMAL DE TRABAJO 1 Consulta de Usuario:			

IDENTIFICADOR CASO DE USO: ADM_02		NOMBRE: Consultar Usuario
Paso	Actor	Sistema
1	Usuario Administrador ingresa a la aplicación	
2		Se solicita Logging
3	Se autentica el Usuario Administrador	
4		Valida los permisos que tiene el usuario y carga la aplicación con el perfil
5	Ingresa a la opción de Consulta	
6		Se despliega el formulario de Consulta
7	Ingresa los parámetros para realizar la consulta del usuario	
8		El sistema verifica que el usuario a consultar existe
9		El sistema trae la información del usuario.
FLUJO Alternativo DE TRABAJO 1 Consulta Usuario No Existe:		
Paso	Actor	Sistema
1	Usuario Administrador ingresa a la aplicación	
2		Se solicita Logging
3	Se autentica el Usuario Administrador	
4		Valida los permisos que tiene el usuario y carga la aplicación con el perfil
5	Ingresa a la opción de Consulta	
6		Se despliega el formulario de Consulta
7	Ingresa los parámetros para realizar la consulta de un usuario inexistente.	
8		El sistema verifica que el usuario a consultar no existe
9		Devuelve mensaje con el resultado de la consulta indicando que el usuario no existe.

IDENTIFICADOR CASO DE USO: ADM_03	NOMBRE: Actualizar Usuario
--	-----------------------------------

IDENTIFICADOR CASO DE USO: ADM_03		NOMBRE: Actualizar Usuario	
CATEGORÍA: Administración			
ACTORES: Usuario Administrador, Sistema			
CASOS DE USO ASOCIADOS: <ul style="list-style-type: none">• Modificar Password.• Actualizar Imagen de Perfil.• Cambiar de estado.			
PROPÓSITO: <ul style="list-style-type: none">• Permite que el usuario administrador actualice la información de un usuario.			
DATOS DE ENTRADA:			
Id.	Nombre	Tipo de Dato	Validaciones
1	Imagen de Perfil	JPG	Imagen correcta
2	Nombres Usuario	String	Longitud, Requerido
3	Apellidos	String	Longitud, Requerido
4	Contraseña	String	Características correctas
5	Confirmación Contraseña	String	Contraseña igual a la anterior
6	Género	String	Una sola Opción
7	Dirección	String	
8	Número Celular	INT	
6	País	String	
10	Estado/Departamento	String	
11	Ciudad	String	
12	Código Postal	INT	Requerido USA
13	Captcha	String	
14	Aceptación de los términos y condiciones del aplicativo.	Boolean	
DATOS DE SALIDA:			
Id.	Nombre	Tipo de Dato	Validaciones
1			
2			
3			
PRECONDICIONES: <ul style="list-style-type: none">• Usuario Administrador debe estar registrado en la aplicación.• Usuario a Actualizar debe estar registrado en la aplicación.			
RESTRICCIONES: <ul style="list-style-type: none">• Usuario Administrador no tiene permisos para hacer la actualización de su información			
CONTROLES: <ul style="list-style-type: none">• Usuario ingresado no existe.• Campos requeridos para guardar el formulario• Si el usuario ingresa contraseña que cumpla con las características.			
FLUJO NORMAL DE TRABAJO 1 Actualización de Usuario:			

IDENTIFICADOR CASO DE USO: ADM_03		NOMBRE: Actualizar Usuario
Paso	Actor	Sistema
1	Usuario Administrador ingresa a la aplicación	
2		Se solicita Logging
	Se autentica el Usuario Administrador	
3		Valida los permisos que tiene el usuario y carga la aplicación con el perfil
4	Ingresa a la opción de Actualizar Usuario	
5		Se despliega el formulario de Actualización
6	Usuario Administrador ingresa el Id Usuario a actualizar	
7		Sistema valida que el Id usuario ingresado exista
8	Usuario actualiza la información que requiere	
9	Se aceptan términos y condiciones	
10		El sistema verifica que los campos requeridos de formulario estén diligenciados
11		Solicita confirmación de la actualización
12	Usuario confirma la actualización	
13		Guarda los cambios realizados en la información
FLUJO Alternativo DE TRABAJO 1 Actualizar Usuario que No Existe:		
Paso	Actor	Sistema
1	Usuario Administrador ingresa a la aplicación	
2		Se solicita Logging
3	Se autentica el Usuario Administrador	
4		Valida los permisos que tiene el usuario y carga la aplicación con el perfil
5	Ingresa a la opción de Actualizar Usuario	
6		Se despliega el formulario de Actualización
7	Usuario Administrador ingresa el Id Usuario a actualizar que no existe	
8		Sistema valida que el Id usuario ingresado no existe
9		Solicita ingresar un usuario existente.

IDENTIFICADOR CASO DE USO: ADM_03		NOMBRE: Cambiar Estado Usuario	
CATEGORÍA: Administración			
ACTORES: Usuario Administrador, Sistema			
CASOS DE USO ASOCIADOS: <ul style="list-style-type: none">• Actualizar Usuario.• Consultar Usuario.			
PROPÓSITO: <ul style="list-style-type: none">• Permitir al usuario administrador activar o desactivar un usuario.			
DATOS DE ENTRADA:			
Id.	Nombre	Tipo de Dato	Validaciones
1	Usuario	String	Usuario Existente
2	Nombres Usuario	String	
3	Apellidos	String	
4	Estado	String	
DATOS DE SALIDA:			
Id.	Nombre	Tipo de Dato	Validaciones
1	Imagen de Perfil	JPG	Información no editable
2	Nombres Usuario	String	Información no editable
3	Apellidos	String	Información no editable
4	Contraseña	String	Información no editable
5	Confirmación Contraseña	String	Información no editable
6	Género	String	Información no editable
7	Dirección	String	Información no editable
8	Número Celular	INT	Información no editable
6	País	String	Información no editable
10	Estado/Departamento	String	Información no editable
11	Ciudad	String	Información no editable
12	Código Postal	INT	Información no editable
13	Captcha	String	Información no editable
14	Aceptación de los términos y condiciones del aplicativo.	Boolean	Información no editable
PRECONDICIONES: <ul style="list-style-type: none">• Usuario Administrador debe estar registrado en la aplicación.• Usuario a cambiar estado debe estar registrado en la aplicación			
RESTRICCIONES: <ul style="list-style-type: none">• Usuario no tiene permisos para hacer la consulta• Usuario no tiene permisos para cambio de estado			
CONTROLES: <ul style="list-style-type: none">•			
FLUJO NORMAL DE TRABAJO 1 Cambiar Estado Usuario Activo:			
Paso	Actor	Sistema	

IDENTIFICADOR CASO DE USO: ADM_03		NOMBRE: Cambiar Estado Usuario
1	Usuario Administrador ingresa a la aplicación	
2		Se solicita Logging
3	Se autentica el Usuario Administrador	
4		Valida los permisos que tiene el usuario y carga la aplicación con el perfil
5	Ingresa a la opción de Consulta Usuario	
6		Se despliega el formulario de Consulta
7	Ingresa los parámetros para realizar la consulta del usuario Activo	
8		El sistema verifica que el usuario a consultar existe
9		El sistema trae la información del usuario.
10	Usuario Administrador selecciona estado inactivo.	
11	Usuario administrador guarda el cambio	
12		Solicita confirmación del cambio.
13	Usuario Administrador confirma el cambio	
14		Guarda el cambio de estado.
FLUJO NORMAL DE TRABAJO 2 Cambiar Estado Usuario In Activo :		
Paso	Actor	Sistema
1	Usuario Administrador ingresa a la aplicación	
2		Se solicita Logging
3	Se autentica el Usuario Administrador	
4		Valida los permisos que tiene el usuario y carga la aplicación con el perfil
5	Ingresa a la opción de Consulta Usuario	
6		Se despliega el formulario de Consulta
7	Ingresa los parámetros para realizar la consulta del usuario Inactivo	
8		El sistema verifica que el usuario a consultar existe
9		El sistema trae la información del usuario.
10	Usuario Administrador selecciona estado activo.	

IDENTIFICADOR CASO DE USO: ADM_03		NOMBRE: Cambiar Estado Usuario
11	Usuario administrador guarda el cambio	
12		Solicita confirmación del cambio.
13	Usuario Administrador confirma el cambio	
14		Guarda el cambio de estado.
FLUJO Alterno DE TRABAJO 1 Consulta Usuario No Existe:		
Paso	Actor	Sistema
1	Usuario Administrador ingresa a la aplicación	
2		Se solicita Logging
3	Se autentica el Usuario Administrador	
4		Valida los permisos que tiene el usuario y carga la aplicación con el perfil
5	Ingresa a la opción de Consulta	
6		Se despliega el formulario de Consulta
7	Ingresa los parámetros para realizar la consulta de un usuario inexistente.	
8		El sistema verifica que el usuario a consultar no existe
9		Devuelve mensaje con el resultado de la consulta indicando que el usuario no existe.

IDENTIFICADOR CASO DE USO: ADM_04		NOMBRE: Crear Grupo	
CATEGORÍA: Administrador			
ACTORES: Usuario Administrador, Sistema			
CASOS DE USO ASOCIADOS: <ul style="list-style-type: none">No aplica			
PROPÓSITO: <ul style="list-style-type: none">Permitir al usuario administrador adicionar en la aplicación un grupo con su información: nombre del grupo y descripción del grupo.			
DATOS DE ENTRADA:			
Id.	Nombre	Tipo de Dato	Validaciones
1	Nombre del Grupo	String	String mayor a 1 carácter
2	Descripción del grupo	String	String mayor a 1 carácter
3	Estado	Boolean	
DATOS DE SALIDA:			
Id.	Nombre	Tipo de Dato	Validaciones
1			
PRECONDICIONES: <ul style="list-style-type: none">Usuario debe estar registrado en la aplicación con el rol de administrador.			
RESTRICCIONES: <ul style="list-style-type: none">El grupo ya existeNombre de grupo invalidoDescripción del grupo invalida			
CONTROLES: <ul style="list-style-type: none">El valor del campo nombre del grupo no debe existir en la aplicación.El valor del campo nombre del grupo no debe ser vacío ni nuloLa valor del campo descripción no debe ser vacío ni nulo.			
FLUJO NORMAL DE TRABAJO 1 Crear Grupo:			
Paso	Actor	Sistema	
1	Usuario administrador accede a la opción de crear grupo.		
2		Despliega el popup para crear grupo	
3	Ingresa Nombre del grupo y descripción del grupo		
4		Valida si la información es correcta	
5		Despliega la confirmación de creación del grupo	
FLUJO Alterno 1 Error en Crear Grupo:			
Paso	Actor	Sistema	
1	Usuario accede a la opción de crear		

IDENTIFICADOR CASO DE USO: ADM_04		NOMBRE: Crear Grupo
	grupo.	
2		Despliega el popup para crear grupo
3	Ingresa Nombre del grupo y descripción del grupo	
4		Identifica que la información ingresada no es valida
5		Despliega un mensaje de error y solicita ingresar nuevamente los datos
6	Usuario ingresa nuevamente los datos	

IDENTIFICADOR CASO DE USO: ADM_05			NOMBRE: Consultar Grupos
CATEGORÍA: Administración			
ACTORES: Usuario Administrador, Sistema			
CASOS DE USO ASOCIADOS: <ul style="list-style-type: none">No aplica			
PROPÓSITO: <ul style="list-style-type: none">Permitir al usuario administrador buscar en la aplicación un grupo ya creado con la información: nombre del grupo.			
DATOS DE ENTRADA:			
Id.	Nombre	Tipo de Dato	Validaciones
1	Nombre del Grupo	String	String mayor a 1 carácter
DATOS DE SALIDA:			
Id.	Nombre	Tipo de Dato	Validaciones
1			
PRECONDICIONES: <ul style="list-style-type: none">Usuario debe estar registrado en la aplicación.			
RESTRICCIONES: <ul style="list-style-type: none">El grupo no existeNombre de grupo invalido			
CONTROLES: <ul style="list-style-type: none">El valor del campo nombre del grupo no debe ser vacío ni nulo			
FLUJO NORMAL DE TRABAJO 1 Consultar Grupo:			
Paso	Actor	Sistema	
1	Usuario accede a la opción de consultar grupo.		
2		Despliega el popup para consultar grupo	
3	Ingresa Nombre del grupo		
4		Valida si la información es correcta	
5		Despliega el resultado de la búsqueda del grupo	
FLUJO Alterno 1 Error en Consultar Grupo:			
Paso	Actor	Sistema	
1	Usuario accede a la opción de consultar grupo.		
2		Despliega el popup para consultar grupo	
3	Ingresa Nombre del grupo		
4		Identifica que la información ingresada no es valida	
5		Despliega un mensaje de error y solicita	

IDENTIFICADOR CASO DE USO: ADM_05		NOMBRE: Consultar Grupos
		ingresar nuevamente los datos
6	Usuario ingresa nuevamente los datos	

IDENTIFICADOR CASO DE USO: ADM_06		NOMBRE: Actualizar Grupo	
CATEGORÍA: Autorización			
ACTORES: Usuario Administrador, Sistema			
CASOS DE USO ASOCIADOS: <ul style="list-style-type: none">Consultar Grupo			
PROPÓSITO: <ul style="list-style-type: none">Permitir al usuario administrador cambiar en la aplicación el nombre del grupo ya creado con la información: nombre del grupo.			
DATOS DE ENTRADA:			
Id.	Nombre	Tipo de Dato	Validaciones
1	Nombre del Grupo	String	String mayor a 1 carácter
DATOS DE SALIDA:			
Id.	Nombre	Tipo de Dato	Validaciones
1			
PRECONDICIONES: <ul style="list-style-type: none">Usuario administrador debe estar registrado en la aplicación.Grupo a Actualizar debe estar creado en la aplicación			
RESTRICCIONES: <ul style="list-style-type: none">El nombre del grupo a actualizar ya existeNombre de grupo invalido			
CONTROLES: <ul style="list-style-type: none">El valor del campo nombre del grupo no debe ser vacío ni nulo			
FLUJO NORMAL DE TRABAJO 1 Actualizar Grupo:			
Paso	Actor	Sistema	
1	Usuario administrador accede a la opción de actualizar grupo.		
2		Despliega el popup para actualizar grupo	
3		Lista los grupos existentes	
4	Selecciona el grupo a Actualizar		
5		Despliega el campo para actualizar el nombre del grupo	
6	Ingresa el nombre del grupo para actualizar		
7		Valida si la información es correcta	
8		Despliega el confirmación de la actualización del grupo	
FLUJO Alterno 1 Error en Actualizar Grupo:			
Paso	Actor	Sistema	
1	Usuario accede a la opción de		

IDENTIFICADOR CASO DE USO: ADM_06		NOMBRE: Actualizar Grupo
	actualizar grupo.	
2		Despliega el popup para actualizar grupo
3		Lista los grupos existentes
4	Selecciona el grupo a Actualizar	
5		Despliega el campo para actualizar el nombre del grupo
6	Ingresa el nombre del grupo para actualizar	
7		Valida que la información ingresada no es correcta
8		Despliega un mensaje de error y solicita ingresar nuevamente los datos
9	Usuario ingresa nuevamente los datos	

IDENTIFICADOR CASO DE USO: ADM_07		NOMBRE: Crear Rol	
CATEGORÍA: Administración			
ACTORES: Usuario Administración, Sistema			
CASOS DE USO ASOCIADOS: <ul style="list-style-type: none">No aplica			
PROPÓSITO: <ul style="list-style-type: none">Permitir al usuario administrador adicionar en la aplicación un Rol con su información: nombre del rol y descripción del rol.			
DATOS DE ENTRADA:			
Id.	Nombre	Tipo de Dato	Validaciones
1	Nombre del Rol	String	String mayor a 1 carácter
2	Descripción del Rol	String	String mayor a 1 carácter
DATOS DE SALIDA:			
Id.	Nombre	Tipo de Dato	Validaciones
1			
PRECONDICIONES: <ul style="list-style-type: none">Usuario debe estar registrado en la aplicación con el rol de administrador.			
RESTRICCIONES: <ul style="list-style-type: none">El rol ya existeNombre de rol invalidoDescripción del rol invalida			
CONTROLES: <ul style="list-style-type: none">El valor del campo nombre del rol no debe existir en la aplicación.El valor del campo nombre del rol no debe ser vacío ni nuloLa valor del campo descripción no debe ser vacío ni nulo.			
FLUJO NORMAL DE TRABAJO 1 Crear Rol:			
Paso	Actor	Sistema	
1	Usuario Administrador accede a la opción de crear rol.		
2		Despliega el popup para crear rol	
3	Ingresa Nombre del rol y descripción del rol		
4		Valida si la información es correcta	
5		Despliega la confirmación de creación del rol	
FLUJO Alterno 1 Error en Crear Rol:			
Paso	Actor	Sistema	
1	Usuario accede a la opción de crear rol.		
2		Despliega el popup para crear rol	

IDENTIFICADOR CASO DE USO: ADM_07		NOMBRE: Crear Rol
3	Ingresa Nombre del rol y descripción del rol	
4		Identifica que la información ingresada no es valida
5		Despliega un mensaje de error y solicita ingresar nuevamente los datos
6	Usuario ingresa nuevamente los datos	

IDENTIFICADOR CASO DE USO: ADM_08			NOMBRE: Consultar Roles		
CATEGORÍA: Administración					
ACTORES: Usuario Administrador, Sistema					
CASOS DE USO ASOCIADOS: <ul style="list-style-type: none">Actualizar Rol					
PROPÓSITO: <ul style="list-style-type: none">Permitir al usuario administrador buscar en la aplicación un rol ya creado con la información: nombre del rol.					
DATOS DE ENTRADA:					
Id.	Nombre		Tipo de Dato	Validaciones	
1	Nombre del Rol		String	String mayor a 1 carácter	
DATOS DE SALIDA:					
Id.	Nombre		Tipo de Dato	Validaciones	
1					
PRECONDICIONES: <ul style="list-style-type: none">Usuario administrador debe estar registrado en la aplicación.Usuario administrador debe tener permisos para consultar el RolRol a consultar ya debe estar creado en la aplicación.					
RESTRICCIONES: <ul style="list-style-type: none">El rol no existeNombre de rol invalido					
CONTROLES: <ul style="list-style-type: none">El valor del campo nombre del rol no debe ser vacío ni nulo					
FLUJO NORMAL DE TRABAJO 1 Consultar roles:					
Paso	Actor			Sistema	
1	Usuario Administrador accede a la opción de consultar rol.				
2				Despliega el popup para buscar rol	
3	Ingresa Nombre del rol				
4				Valida si la información es correcta	
5				Despliega el resultado de la consulta del rol.	
FLUJO Alterno 1 Error en Consultar Roles:					
Paso	Actor			Sistema	
1	Usuario administrador accede a la opción de consultar rol.				
2				Despliega el popup para buscar rol	
3	Ingresa Nombre del rol				
4				Valida la información ingresada no es correcta	

IDENTIFICADOR CASO DE USO: ADM_08		NOMBRE: Consultar Roles
5		Despliega un error y solicita al usuario ingresar nuevamente los datos.
6	Usuario administrador ingresa nuevamente los datos	

IDENTIFICADOR CASO DE USO: ADM_09			NOMBRE: Actualizar Roles		
CATEGORÍA: Administración					
ACTORES: Usuario Administrador, Sistema					
CASOS DE USO ASOCIADOS: <ul style="list-style-type: none">Consulta de Roles					
PROPÓSITO: <ul style="list-style-type: none">Permitir al usuario cambiar en la aplicación el nombre del rol ya creado con la información: nombre del rol.					
DATOS DE ENTRADA:					
Id.	Nombre		Tipo de Dato	Validaciones	
1	Nombre del Rol		String	String mayor a 1 carácter	
DATOS DE SALIDA:					
Id.	Nombre		Tipo de Dato	Validaciones	
1					
PRECONDICIONES: <ul style="list-style-type: none">Usuario Administrador debe estar registrado en la aplicación.Usuario debe tener permisos de modificar roles.El rol a actualizar debe existir en la aplicación.					
RESTRICCIONES: <ul style="list-style-type: none">El nombre del rol a actualizar ya existeNombre de rol invalido					
CONTROLES: <ul style="list-style-type: none">El valor del campo nombre del rol no debe ser vacío ni nulo					
FLUJO NORMAL DE TRABAJO 1 Actualizar Roles:					
Paso	Actor			Sistema	
1	Usuario administrador accede a la opción de actualizar rol.				
2				Despliega el popup para actualizar rol	
3				Lista los roles existentes	
4	Selecciona el rol a Actualizar				
5				Despliega el campo para actualizar el nombre del rol	
6	Ingresa el nombre del rol para actualizar				
7				Valida si la información es correcta	
8				Despliega el confirmación de la actualización del rol	
FLUJO Alterno 1 Error en Actualizar Roles:					
Paso	Actor			Sistema	

IDENTIFICADOR CASO DE USO: ADM_09		NOMBRE: Actualizar Roles
1	Usuario Administrador accede a la opción de actualizar rol.	
2		Despliega el popup para actualizar rol
3		Lista los roles existentes
4	Selecciona el rol a Actualizar	
5		Despliega el campo para actualizar el nombre del rol
6	Ingresa el nombre del rol para actualizar	
7		Valida que la información ingresada no es correcta
8		Despliega un mensaje de error y solicita ingresar nuevamente los datos
9	Usuario ingresa nuevamente los datos	

IDENTIFICADOR CASO DE USO: ADM_10		NOMBRE: Crear Permiso	
CATEGORÍA: Administración			
ACTORES: Usuario Administración, Sistema			
CASOS DE USO ASOCIADOS: <ul style="list-style-type: none">No aplica			
PROPÓSITO: <ul style="list-style-type: none">Permitir al usuario administrador adicionar en la aplicación un permiso			
DATOS DE ENTRADA:			
Id.	Nombre	Tipo de Dato	Validaciones
1	Nombre del Permiso	String	String mayor a 1 carácter
2	Descripción del Permiso	String	String mayor a 1 carácter
3	Estado	Boolean	
DATOS DE SALIDA:			
Id.	Nombre	Tipo de Dato	Validaciones
1			
PRECONDICIONES: <ul style="list-style-type: none">Usuario Administrador debe estar registrado en la aplicación con el rol de administrador.Usuario Administrador debe tener permisos para crear permisos.El permiso a crear no existe			
RESTRICCIONES: <ul style="list-style-type: none">El permiso ya existeNombre de permiso invalidoDescripción del permiso invalida			
CONTROLES: <ul style="list-style-type: none">El valor del campo nombre del permiso no debe existir en la aplicación.El valor del campo nombre del permiso no debe ser vacío ni nuloLa valor del campo descripción no debe ser vacío ni nulo.			
FLUJO NORMAL DE TRABAJO 1 Crear Permiso:			
Paso	Actor	Sistema	
1	Usuario Administrador accede a la opción de crear permiso.		
2		Despliega el popup para crear permiso	
3	Ingresa Nombre del permiso y descripción del permiso		
4		Valida si la información es correcta	
5		Despliega la confirmación de creación del permiso	
FLUJO Alterno 1 Error en Crear Rol: Permiso ya Existe			
Paso	Actor	Sistema	

IDENTIFICADOR CASO DE USO: ADM_10		NOMBRE: Crear Permiso
1	Usuario Administrador accede a la opción de crear permiso.	
2		Despliega el popup para crear permiso
3	Ingresa Nombre del permiso ya existente y descripción del permiso	
4		Identifica que la información ingresada no es valida
5		Despliega un mensaje de error y solicita ingresar nuevamente los datos
6	Usuario administrador ingresa nuevamente los datos	

IDENTIFICADOR CASO DE USO: ADM_11		NOMBRE: Consultar Permisos	
CATEGORÍA: Administración			
ACTORES: Usuario Administrador, Sistema			
CASOS DE USO ASOCIADOS: <ul style="list-style-type: none">Actualizar Permiso			
PROPÓSITO: <ul style="list-style-type: none">Permitir al usuario administrador buscar en la aplicación un permiso ya creado.			
DATOS DE ENTRADA:			
Id.	Nombre	Tipo de Dato	Validaciones
1	Nombre del permiso	String	String mayor a 1 carácter
DATOS DE SALIDA:			
Id.	Nombre	Tipo de Dato	Validaciones
1			
PRECONDICIONES: <ul style="list-style-type: none">Usuario administrador debe estar registrado en la aplicación.Usuario administrador debe tener permisos para consultar el permisoPermiso a consultar ya debe estar creado en la aplicación.			
RESTRICCIONES: <ul style="list-style-type: none">El permiso no existe			
CONTROLES: <ul style="list-style-type: none">El valor del campo nombre del permiso no debe ser vacío ni nulo			
FLUJO NORMAL DE TRABAJO 1 Consultar Permiso:			
Paso	Actor	Sistema	
1	Usuario Administrador accede a la opción de consultar permiso.		
2		Despliega el popup para buscar permiso	
3	Ingresa Nombre del permiso		
4		Valida si la información es correcta	
5		Despliega el resultado de la consulta del permiso.	
FLUJO Alterno 1 Error en Consultar Permisos: Permiso no Existe			
Paso	Actor	Sistema	
1	Usuario administrador accede a la opción de consultar permiso.		
2		Despliega el popup para buscar permiso	
3	Ingresa Nombre de un permiso que no existe		
4		Valida que el nombre del permiso no es correcto	

IDENTIFICADOR CASO DE USO: ADM_11		NOMBRE: Consultar Permisos
5		Despliega un error y solicita al usuario ingresar nuevamente los datos.
6	Usuario administrador ingresa nuevamente los datos	

IDENTIFICADOR CASO DE USO: ADM_12		NOMBRE: Actualizar Permiso	
CATEGORÍA: Administración			
ACTORES: Usuario Administrador, Sistema			
CASOS DE USO ASOCIADOS: <ul style="list-style-type: none">Consulta de permiso			
PROPÓSITO: <ul style="list-style-type: none">Permitir al usuario actualizar en la aplicación un permiso			
DATOS DE ENTRADA:			
Id.	Nombre	Tipo de Dato	Validaciones
1	Nombre del permiso	String	String mayor a 1 carácter
DATOS DE SALIDA:			
Id.	Nombre	Tipo de Dato	Validaciones
1			
PRECONDICIONES: <ul style="list-style-type: none">Usuario Administrador debe estar registrado en la aplicación.Usuario debe tener permisos de modificar permisos.El permiso a actualizar debe existir en la aplicación.			
RESTRICCIONES: <ul style="list-style-type: none">El nombre del permiso a actualizar ya existeNombre de permiso invalido			
CONTROLES: <ul style="list-style-type: none">El valor del campo nombre del permiso no debe ser vacío ni nulo			
FLUJO NORMAL DE TRABAJO 1 Actualizar Permiso:			
Paso	Actor	Sistema	
1	Usuario administrador accede a la opción de actualizar permiso.		
2		Despliega el popup para actualizar permiso	
3		Lista los permisos existentes	
4	Selecciona el permiso a Actualizar		
5		Despliega el formulario para actualizar el permiso	
6	Ingresa la información del permiso a actualizar		
7		Valida si la información es correcta	
8		Despliega el confirmación de la actualización del permiso	
FLUJO Alterno 1 Error en Actualizar Permiso:			
Paso	Actor	Sistema	
1	Usuario Administrador accede a la opción de actualizar permiso.		

IDENTIFICADOR CASO DE USO: ADM_12		NOMBRE: Actualizar Permiso
2		Despliega el popup para actualizar permiso
3		Lista los permisos existentes
4	Selecciona el permiso a Actualizar	
5		Despliega el formulario para modificar el permiso
6	Ingresar el nombre del permiso para actualizar	
7		Valida que la información ingresada no es correcta
8		Despliega un mensaje de error y solicita ingresar nuevamente los datos
9	Usuario administrador ingresa nuevamente los datos	

IDENTIFICADOR CASO DE USO: ADM_13		NOMBRE: Crear Tipo de Recurso	
CATEGORÍA: Administración			
ACTORES: Usuario Administración, Sistema			
CASOS DE USO ASOCIADOS: <ul style="list-style-type: none">Actualizar Tipo de Recurso			
PROPÓSITO: <ul style="list-style-type: none">Permitir al usuario administrador adicionar en la aplicación un Tipo de Recurso			
DATOS DE ENTRADA:			
Id.	Nombre	Tipo de Dato	Validaciones
1	Nombre del Tipo de Recurso	String	String mayor a 1 carácter
2	Descripción del Tipo de Recurso	String	String mayor a 1 carácter
3	Estado	Boolean	
4	Ruta Relativa	String	
DATOS DE SALIDA:			
Id.	Nombre	Tipo de Dato	Validaciones
1			
PRECONDICIONES: <ul style="list-style-type: none">Usuario Administrador debe estar registrado en la aplicación con el rol de administrador.Usuario Administrador debe tener permisos para crear Tipo de Recursos.El Tipo de Recurso a crear no existe			
RESTRICCIONES: <ul style="list-style-type: none">El Tipo de Recurso ya existeNombre del Tipo de Recurso invalidoDescripción del Tipo de Recurso invalidaRuta Relativa invalida			
CONTROLES: <ul style="list-style-type: none">El valor del campo nombre del Tipo de Recurso no debe existir en la aplicación.El valor del campo nombre del Tipo de Recurso no debe ser vacío ni nuloEl valor del campo descripción no debe ser vacío ni nulo.El valor del campo de ruta relativa no debe ser vacío ni nulo.			
FLUJO NORMAL DE TRABAJO 1 Crear Tipo de Recurso			
Paso	Actor	Sistema	
1	Usuario Administrador accede a la opción de crear Tipo de Recurso.		
2		Despliega el popup para crear Tipo de Recurso	
3	Ingresa Nombre del Tipo de Recurso y descripción del Tipo de Recurso		

IDENTIFICADOR CASO DE USO: ADM_13		NOMBRE: Crear Tipo de Recurso
4		Valida si la información es correcta
5		Despliega la confirmación de creación del Tipo de Recurso
FLUJO Alterno 1 Error en Crear Rol: Permiso ya Existe		
Paso	Actor	Sistema
1	Usuario Administrador accede a la opción de crear Tipo de Recurso.	
2		Despliega el popup para crear Tipo de Recurso
3	Ingresa Nombre del Tipo de Recurso ya existente y descripción del Tipo de Recurso	
4		Identifica que la información ingresada no es valida
5		Despliega un mensaje de error y solicita ingresar nuevamente los datos
6	Usuario administrador ingresa nuevamente los datos	

IDENTIFICADOR CASO DE USO: ADM_14		NOMBRE: Consultar Tipo de Recurso	
CATEGORÍA: Administración			
ACTORES: Usuario Administrador, Sistema			
CASOS DE USO ASOCIADOS: <ul style="list-style-type: none">Actualizar Permiso			
PROPÓSITO: <ul style="list-style-type: none">Permitir al usuario administrador buscar en la aplicación un Tipo de Recurso ya creado.			
DATOS DE ENTRADA:			
Id.	Nombre	Tipo de Dato	Validaciones
1	Nombre del Tipo de Recurso.	String	String mayor a 1 carácter
DATOS DE SALIDA:			
Id.	Nombre	Tipo de Dato	Validaciones
1			
PRECONDICIONES: <ul style="list-style-type: none">Usuario administrador debe estar registrado en la aplicación.Usuario administrador debe tener permisos para consultar el Tipo de RecursoEl Tipo de Recurso a consultar ya debe estar creado en la aplicación.			
RESTRICCIONES: <ul style="list-style-type: none">El Tipo de Recurso no existe			
CONTROLES: <ul style="list-style-type: none">El valor del campo nombre del Tipo de Recurso no debe ser vacío ni nulo			
FLUJO NORMAL DE TRABAJO 1 Consultar Tipo de Recurso:			
Paso	Actor	Sistema	
1	Usuario Administrador accede a la opción de consultar Tipo de Recurso.		
2		Despliega el popup para buscar Tipo de Recurso	
3	Ingresa Nombre del Tipo de Recurso		
4		Valida si la información es correcta	
5		Despliega el resultado de la consulta del Tipo de Recurso	
FLUJO Alterno 1 Error en Consultar Permisos: Tipo de Recurso no Existe			
Paso	Actor	Sistema	
1	Usuario administrador accede a la opción de consultar Tipo de Permiso		
2		Despliega el popup para buscar Tipo de Recurso	
3	Ingresa Nombre de un Tipo de		

IDENTIFICADOR CASO DE USO: ADM_14		NOMBRE: Consultar Tipo de Recurso
	Recurso que no existe	
4		Valida que el nombre del Tipo de Recurso no es correcto
5		Despliega un error y solicita al usuario ingresar nuevamente los datos.
6	Usuario administrador ingresa nuevamente los datos	

IDENTIFICADOR CASO DE USO: ADM_15		NOMBRE: Actualizar Tipo de Recurso	
CATEGORÍA: Administración			
ACTORES: Usuario Administrador, Sistema			
CASOS DE USO ASOCIADOS: <ul style="list-style-type: none">Consulta de Tipo de Recurso			
PROPÓSITO: <ul style="list-style-type: none">Permitir al usuario actualizar en la aplicación un Tipo de Recurso			
DATOS DE ENTRADA:			
Id.	Nombre	Tipo de Dato	Validaciones
1	Nombre del Tipo de Recurso	String	String mayor a 1 carácter
DATOS DE SALIDA:			
Id.	Nombre	Tipo de Dato	Validaciones
1			
PRECONDICIONES: <ul style="list-style-type: none">Usuario Administrador debe estar registrado en la aplicación.Usuario debe tener permisos de modificar Tipo de Recurso.El Tipo de recurso a actualizar debe existir en la aplicación.			
RESTRICCIONES: <ul style="list-style-type: none">El nombre del Tipo de Recurso a actualizar ya existeNombre de Tipo de Recurso invalido			
CONTROLES: <ul style="list-style-type: none">El valor del campo nombre del Tipo de Recurso no debe ser vacío ni nulo			
FLUJO NORMAL DE TRABAJO 1 Actualizar Tipo de Recurso:			
Paso	Actor	Sistema	
1	Usuario administrador accede a la opción de actualizar Tipo de Recurso		
2		Despliega el popup para actualizar Tipo de Recurso	
3		Lista los Tipos de Recursos existentes	
4	Selecciona el Tipo de Recurso a Actualizar		
5		Despliega el formulario para actualizar el Tipo de Recurso	
6	Ingresa la información del Tipo de Recurso a actualizar		
7		Valida si la información es correcta	
8		Despliega el confirmación de la actualización del Tipo de Recurso	
FLUJO Alterno 1 Error en Actualizar Tipo de Recurso:			

IDENTIFICADOR CASO DE USO: ADM_15		NOMBRE: Actualizar Tipo de Recurso
Paso	Actor	Sistema
1	Usuario Administrador accede a la opción de actualizar Tipo de Recurso.	
2		Despliega el popup para actualizar Tipo de Recurso
3		Lista los Tipos de Recursos existentes
4	Selecciona el Tipo de Recurso a Actualizar	
5		Despliega el formulario para modificar el Tipo de Recurso
6	Ingresar el nombre del Tipo de Recurso para actualizar	
7		Valida que la información ingresada no es correcta
8		Despliega un mensaje de error y solicita ingresar nuevamente los datos
9	Usuario administrador ingresa nuevamente los datos	

IDENTIFICADOR CASO DE USO: ADM_16		NOMBRE: Consultar Acción	
CATEGORÍA: Administración			
ACTORES: Usuario Administrador, Sistema			
CASOS DE USO ASOCIADOS: <ul style="list-style-type: none">No Aplica			
PROPÓSITO: <ul style="list-style-type: none">Permitir al usuario administrador buscar en la aplicación una acción			
DATOS DE ENTRADA:			
Id.	Nombre	Tipo de Dato	Validaciones
1	Nombre de la acción	String	String mayor a 1 carácter
DATOS DE SALIDA:			
Id.	Nombre	Tipo de Dato	Validaciones
1			
PRECONDICIONES: <ul style="list-style-type: none">Usuario administrador debe estar registrado en la aplicación.Usuario administrador debe tener permisos para consultar acciones			
RESTRICCIONES: <ul style="list-style-type: none">			
CONTROLES: <ul style="list-style-type: none">El valor del campo nombre de la acción no debe ser vacío ni nulo			
FLUJO NORMAL DE TRABAJO 1 Consultar Acción:			
Paso	Actor	Sistema	
1	Usuario Administrador accede a la opción de consultar Acción.		
2		Despliega el popup para buscar Acción	
3	Ingresa Nombre de la Acción		
4		Valida si la información es correcta	
5		Despliega el resultado de la consulta de acciones	

IDENTIFICADOR CASO DE USO: ADM_17		NOMBRE: Agregar Rol a Grupo	
CATEGORÍA: Administración			
ACTORES: Usuario Administrador, Sistema			
CASOS DE USO ASOCIADOS: <ul style="list-style-type: none">No Aplica			
PROPÓSITO: <ul style="list-style-type: none">Permitir al usuario administrador agregar Roles a un grupo.			
DATOS DE ENTRADA:			
Id.	Nombre	Tipo de Dato	Validaciones
1	Nombre del Rol	String	String mayor a 1 carácter
DATOS DE SALIDA:			
Id.	Nombre	Tipo de Dato	Validaciones
1			
PRECONDICIONES: <ul style="list-style-type: none">Usuario administrador debe estar registrado en la aplicación.Usuario administrador debe tener permisos para agregar Rol a Grupo			
RESTRICCIONES: <ul style="list-style-type: none">No Aplica			
CONTROLES: <ul style="list-style-type: none">EL Rol a agregar al grupo no debe estar agregado previamente.			
FLUJO NORMAL DE TRABAJO 1: Agregar Rol a Grupo			
Paso	Actor	Sistema	
1	Usuario Administrador accede a la opción de Actualizar Grupo.		
2	Da clic en el botón de Agregar Rol		
3		Carga la lista de Roles existentes en la aplicación.	
4	Selecciona los roles que desea agregar al grupo.		
5	Da clic en el botón agregar roles		
		Guarda el cabio realizado	

IDENTIFICADOR CASO DE USO: ADM_18	NOMBRE: Agregar Usuario a Grupo
--	--

IDENTIFICADOR CASO DE USO: ADM_18			NOMBRE: Agregar Usuario a Grupo		
CATEGORÍA: Administración					
ACTORES: Usuario Administrador, Sistema					
CASOS DE USO ASOCIADOS: <ul style="list-style-type: none">No Aplica					
PROPÓSITO: <ul style="list-style-type: none">Permitir al usuario administrador agregar Usuario a un grupo.					
DATOS DE ENTRADA:					
Id.	Nombre		Tipo de Dato	Validaciones	
1	Nombre del Usuario		String	String mayor a 1 carácter	
DATOS DE SALIDA:					
Id.	Nombre		Tipo de Dato	Validaciones	
1					
PRECONDICIONES: <ul style="list-style-type: none">Usuario administrador debe estar registrado en la aplicación.Usuario administrador debe tener permisos para agregar Usuario a Grupo					
RESTRICCIONES: <ul style="list-style-type: none">No Aplica					
CONTROLES: <ul style="list-style-type: none">EL Usuario a agregar al grupo no debe estar agregado previamente.El Usuario a agregar al grupo debe tener un rol asignado.					
FLUJO NORMAL DE TRABAJO 1: Agregar Usuario a Grupo					
Paso	Actor			Sistema	
1	Usuario Administrador accede a la opción de Actualizar Grupo.				
2	Da clic en el botón de Agregar Usuario				
3				Carga la lista de Usuarios existentes en la aplicación.	
4	Selecciona los Usuarios que desea agregar al grupo.				
5	Da clic en el botón agregar Usuarios				
				Guarda el cabio realizado	

IDENTIFICADOR CASO DE USO: ADM_19	NOMBRE: Agregar Rol a Usuario
CATEGORÍA: Administración	

IDENTIFICADOR CASO DE USO: ADM_19		NOMBRE: Agregar Rol a Usuario	
ACTORES: Usuario Administrador, Sistema			
CASOS DE USO ASOCIADOS: <ul style="list-style-type: none">No Aplica			
PROPÓSITO: <ul style="list-style-type: none">Permitir al usuario administrador agregar un usuario a un rol			
DATOS DE ENTRADA:			
Id.	Nombre	Tipo de Dato	Validaciones
1	Nombre del Usuario	String	String mayor a 1 carácter
DATOS DE SALIDA:			
Id.	Nombre	Tipo de Dato	Validaciones
1			
PRECONDICIONES: <ul style="list-style-type: none">Usuario administrador debe estar registrado en la aplicación.Usuario administrador debe tener permisos para agregar Usuario a rol			
RESTRICCIONES: <ul style="list-style-type: none">No Aplica			
CONTROLES: <ul style="list-style-type: none">EL Usuario a agregar al rol no debe estar agregado previamente.			
FLUJO NORMAL DE TRABAJO 1: Agregar Usuario a Grupo			
Paso	Actor	Sistema	
1	Usuario Administrador accede a la opción de Actualizar Rol.		
2	Da clic en el botón de Agregar Usuario		
3		Carga la lista de Usuarios existentes en la aplicación.	
4	Selecciona los Usuarios que desea agregar al rol.		
5	Da clic en el botón agregar Usuarios		
		Guarda el cabio realizado	

MÓDULO APLICACIÓN ADA

IDENTIFICADOR CASO DE USO: API_01	NOMBRE: Crear Aplicación
CATEGORÍA: Aplicación	

IDENTIFICADOR CASO DE USO: API_01			NOMBRE: Crear Aplicación
ACTORES: Usuario Administrador, Sistema			
CASOS DE USO ASOCIADOS: <ul style="list-style-type: none">No Aplica			
PROPÓSITO: <ul style="list-style-type: none">Permitir al usuario administrador crear una nueva aplicación			
DATOS DE ENTRADA:			
Id.	Nombre	Tipo de Dato	Validaciones
1	Nombre de la acción	String	String mayor a 1 carácter
2	Correo	String	String mayor a 1 carácter
3	Encabezado	String	String mayor a 1 carácter
4	Pie de pagina	String	String mayor a 1 carácter
5	Hereda de otra aplicación	Checkbox	No aplica
DATOS DE SALIDA:			
Id.	Nombre	Tipo de Dato	Validaciones
1			
PRECONDICIONES: <ul style="list-style-type: none">Usuario administrador debe estar registrado en la aplicación.Usuario administrador debe tener permisos para crear aplicaciones.			
RESTRICCIONES: <ul style="list-style-type: none">			
CONTROLES: <ul style="list-style-type: none">El valor del campo nombre de la aplicación no debe ser vacío ni nulo.El valor del campo correo no debe ser vacío ni nulo.El valor del campo encabezado no de ser vacío ni nulo.El valor del campo pie de página no deber ser vacío ni nulo.			
FLUJO NORMAL DE TRABAJO 1 Crear Aplicación:			
Paso	Actor	Sistema	
1	Usuario Administrador accede a la opción de crear aplicación.		
2		Despliega el formulario de crear aplicación.	
3	Ingresa los datos requeridos para crear la aplicación.		
4		Valida si la información es correcta	
5		Despliega el resultado de la creación de la aplicación.	
FLUJO ALTERNO DE TRABAJO 1 Crear Aplicación:			
Paso	Actor	Sistema	
1	Usuario Administrador accede a la opción de crear aplicación.		
2		Despliega el formulario de crear aplicación.	
3	Ingresa los datos requeridos para		

IDENTIFICADOR CASO DE USO: API_01		NOMBRE: Crear Aplicación
	crear la aplicación.	
4		Valida que la información ingresada no es correcta.
5		Muestra un mensaje de error
6		Solicita al usuario ingresar nuevamente la información.
7	Ingresa los datos requeridos para crear la aplicación.	
8		Despliega el resultado de la creación de la aplicación.

IDENTIFICADOR CASO DE USO: API_02		NOMBRE: Consultar Aplicación	
CATEGORÍA: Aplicación			
ACTORES: Usuario Administrador, Sistema			
CASOS DE USO ASOCIADOS: <ul style="list-style-type: none">No Aplica			
PROPÓSITO: <ul style="list-style-type: none">Permitir al usuario administrador consultar una aplicación ya creada			
DATOS DE ENTRADA:			
Id.	Nombre	Tipo de Dato	Validaciones
1	Nombre de la acción	String	String mayor a 1 carácter
DATOS DE SALIDA:			
Id.	Nombre	Tipo de Dato	Validaciones
1			
PRECONDICIONES: <ul style="list-style-type: none">Usuario administrador debe estar registrado en la aplicación.Usuario administrador debe tener permisos para consultar aplicaciones.			
RESTRICCIONES: <ul style="list-style-type: none">			
CONTROLES: <ul style="list-style-type: none">El valor del campo nombre de la aplicación no debe ser vacío ni nulo.			
FLUJO NORMAL DE TRABAJO 1 Consultar Aplicación:			
Paso	Actor	Sistema	
1	Usuario Administrador accede a la opción de consultar aplicación.		
2		Despliega el formulario de consultar aplicación.	
3	Ingresa el dato requerido para consultar la aplicación.		
4		Valida si la información es correcta	
5		Despliega el resultado de la consulta de la aplicación.	
FLUJO ALTERNO DE TRABAJO 1 Consultar Aplicación:			
Paso	Actor	Sistema	
1	Usuario Administrador accede a la opción de consultar aplicación.		
2		Despliega el formulario de consultar aplicación.	
3	Ingresa el dato requerido para consultar la aplicación.		
4		Valida que la información ingresada no es correcta.	

IDENTIFICADOR CASO DE USO: API_02		NOMBRE: Consultar Aplicación
5		Muestra un mensaje de error
6		Solicita al usuario ingresar nuevamente la información.
7	Ingresa el dato requerido para consultar la aplicación.	
8		Despliega el resultado de la consulta de la aplicación.

IDENTIFICADOR CASO DE USO: API_03		NOMBRE: Actualizar Aplicación	
CATEGORÍA: Aplicación			
ACTORES: Usuario Administrador, Sistema			
CASOS DE USO ASOCIADOS: <ul style="list-style-type: none">No Aplica			
PROPÓSITO: <ul style="list-style-type: none">Permitir al usuario administrador actualizar una aplicación ya creada			
DATOS DE ENTRADA:			
Id.	Nombre	Tipo de Dato	Validaciones
1	Nombre de la acción	String	String mayor a 1 carácter
2	Correo	String	String mayor a 1 carácter
3	Encabezado	String	String mayor a 1 carácter
4	Pie de pagina	String	String mayor a 1 carácter
5	Hereda de otra aplicación	Checkbox	No aplica
DATOS DE SALIDA:			
Id.	Nombre	Tipo de Dato	Validaciones
1			
PRECONDICIONES: <ul style="list-style-type: none">Usuario administrador debe estar registrado en la aplicación.Usuario administrador debe tener permisos para actualizar aplicaciones.			
RESTRICCIONES: <ul style="list-style-type: none">			
CONTROLES: <ul style="list-style-type: none">El valor del campo nombre de la aplicación no debe ser vacío ni nulo.El valor del campo correo no debe ser vacío ni nulo.El valor del campo encabezado no de ser vacío ni nulo.El valor del campo pie de página no deber ser vacío ni nulo.			
FLUJO NORMAL DE TRABAJO 1 Consultar Aplicación:			
Paso	Actor	Sistema	
1	Usuario Administrador accede a la opción de actualizar aplicación.		
2		Despliega el formulario de actualizar aplicación.	
3	Ingresa los datos para actualizar la aplicación.		
4		Valida si la información es correcta	
5		Despliega el resultado de la actualización de la aplicación.	
FLUJO ALTERNO DE TRABAJO 1 Actualizar Aplicación:			
Paso	Actor	Sistema	
1	Usuario Administrador accede a la		

IDENTIFICADOR CASO DE USO: API_03		NOMBRE: Actualizar Aplicación
	opción de actualizar aplicación.	
2		Despliega el formulario de actualizar aplicación.
3	Ingresa los datos para actualizar la aplicación.	
4		Valida que la información ingresada no es correcta.
5		Muestra un mensaje de error
6		Solicita al usuario ingresar nuevamente la información.
7	Ingresa el dato requerido para actualizar la aplicación.	
8		Despliega el resultado de la actualización de la aplicación.

2. Diseño Casos de Prueba

ADA				
Id	Escenario	Id caso de prueba	Caso de prueba	Resultado esperado
1	Inicio Sesión Básico	1.1	Ingresar usuario que este registrado con contraseña correcta	Acceso a la aplicación
		1.2	Ingresar usuario que este registrado con contraseña incorrecta	No permite ingreso a la aplicación, solicita ingresar de nuevo datos.
		1.3	Ingresar usuario que no se encuentre registrado con contraseña correcta	No permite ingreso a la aplicación, solicita ingresar de nuevo datos.
		1.4	Ingresar usuario que este registrado pero que no se encuentre activo	No permite ingreso a la aplicación y aparece mensaje de error
		1.5	Ingreso erróneo de contraseña por tres ocasiones seguidas	Se bloquea usuario, debe solicitar reseteo de contraseña
			Ingresar usuario que este registrado y campo contraseña en blanco	Muestra mensaje de error solicitando contraseña valida
2	Inicio de Sesión con Redes Sociales	2.1	Seleccionar a red social registrada	Carga el acceso a la red social y valida la sesión, e ingresa a aplicación
		2.2	Seleccionar a red social no registrada	No permite ingreso y se debe seleccionar red social o registrarse en la aplicación
3	Modificar Password	3.1	Ingresar contraseña actual, nueva y confirmación valida	Contraseña modificada exitosamente
		3.2	Ingresar contraseña actual, nueva valida, confirmación distinta	Muestra mensaje de error en campo confirmación contraseña se debe volver a digitar
		3.3	Ingresar contraseña actual invalida, nueva valida, confirmación valida	Muestra mensaje de error en campo contraseña actual
		3.4	Ingresar contraseña actual, nueva y confirmación iguales pero no cumple características	Muestra mensaje de error, se debe volver a ingresar contraseña con características validas
		3.5	Ingresar contraseña actual, nueva y confirmación no ingresar nada	Muestra mensaje de error en donde debe agregar contraseña con datos validos

4	Actualizar Datos	4.1	Actualizar campos con parámetros requeridos de Imagen, Nombres Usuario, Apellidos, Contraseña, Confirmación contraseña, Género, Dirección, Número celular, País, Estado Departamento, Ciudad, Código Postal Aceptación de los términos y condiciones aplicativo	Actualizar datos correctamente
		4.2	Actualizar el campo Número de celular	Se actualizará de forma correcta el campo Número de celular, los demás campos no sufrirán ningún cambio.
		4.3	Ubique el campo Términos y Condiciones, desmárquelo y verifique que no permita guardar los cambios.	No permitirá guardar el cambio ya que este campo es requerido.
5	Actualizar Imagen de Perfil	5.1	Ingrese a la información del perfil, ubique la imagen de perfil y modifíquela	La aplicación permitirá la modificación de la imagen de perfil.
		5.2	Ingrese a la información del perfil, ubique la imagen de perfil y elimínela	La aplicación permitirá la eliminación de la imagen y guardará los cambios.
		5.3	Ingrese a la información de perfil, ubique la imagen de perfil, ingrese a modificarla y cancele la acción.	El sistema no guardará ningún cambio sobre la imagen de perfil.
	Cierre de Sesión	6.1	Ubique el link para cerrar la sesión de clic en el y confirme el cierre de la sesión.	La aplicación permitirá el cierre de la sesión del usuario.
		6.2	Ubique el link para cerrar la sesión de clic en el y cancele el cierre de la sesión.	La aplicación no cerrará la sesión y mantendrá al usuario conectado.
		6.3	verifique el tiempo parametrizado para el cierre de sesión por inactividad del usuario, espere el tiempo sin hacer ninguna acción en la pantalla, luego de cumplir el tiempo realice una acción.	El sistema habrá cerrado de forma automática la sesión y solicitará loguearse de nuevo.
7	Crear Usuario	7.1	Ingresar como administrador la información básica de un usuario para registrarlo en la aplicación	La aplicación muestra un mensaje de creación exitosa para el usuario y lo crea en la aplicación

		7.2	Ingresar como administrador la información básica de un usuario con contraseña que no cumple los requisitos para registrarlo en la aplicación	La aplicación muestra un mensaje que error informando que la contraseña no cumple los requisitos
		7.3	Ingresar como administrador la información básica de un usuario ya existente para registrarlo en la aplicación	La aplicación muestra un mensaje de error y solicita ingresar un nuevo ID Usuario
		7.4	Ingresar como administrador la información básica de un usuario para registrarlo en la aplicación con el nombre en blanco	La aplicación muestra un mensaje de error por campo requerido y solicita ingresar un nombre de más de un carácter no nulo ni vacío
8	Consultar Usuario	8.1	Consulta la información como administrador de un usuario ya existente en la aplicación	La aplicación muestra la información del usuario consultado
		8.2	Consulta la información como administrador de un usuario no existente en la aplicación	La aplicación muestra un mensaje de error y solicita ingresar un usuario que se encuentre en el sistema
		8.3	Consulta la información como administrador de un usuario dejando el campo de ID Usuario en blanco	La aplicación muestra un mensaje de error y solicita ingresar un usuario que se encuentre en el sistema con ID de usuario de más de un carácter no nulo ni vacío
9	Actualizar Usuario	9.1	Actualizar la información como administrador de un usuario existente en la aplicación	La aplicación permite actualizar la información del usuario
		9.2	Actualizar la información como administrador de un usuario no existente en la aplicación	La aplicación muestra un mensaje de error y solicita ingresar un usuario que se encuentre en el sistema
		9.3	Actualizar la información como administrador de un usuario dejando el campo de ID Usuario en blanco	La aplicación muestra un mensaje de error y solicita ingresar un usuario que se encuentre en el sistema con ID de usuario de más de un carácter no nulo ni vacío
		9.4	Actualizar la información como administrador de un usuario existente en la aplicación con una contraseña que no cumpla los requisitos	La aplicación muestra un mensaje de error por requisitos no validos y solicita ingresar una contraseña que cumpla los requisitos
10	Cambiar Estado Usuario	10.1	Cambiar el estado como administrador de un usuario existente en en la aplicación	La aplicación permite cambiar el estado del usuario
		10.2	Cambiar el estado como administrador de un usuario no existente en la aplicación	La aplicación muestra un mensaje de error y solicita ingresar un usuario existente en la aplicación

		10.3	Cambiar el estado como administrador de un usuario existente en la aplicación dejando el cambio ID de usuario en blanco	La aplicación muestra un mensaje de error y solicita ingresar un usuario que se encuentre en el sistema con ID de usuario de más de un carácter no nulo ni vacío
		10.4	Cambiar el estado como administrador de un usuario existente en la aplicación que se encuentre inactivo	La aplicación muestra un mensaje diciendo que el usuario ya se encuentra inactivo y no se realiza modificación de los datos
11	Crear Grupo	11.1	Crear un grupo como administrador en la aplicación	La aplicación permite crear un grupo
		11.2	Crear un grupo como administrador ya existente en la aplicación	La aplicación muestra un mensaje diciendo que el grupo ya se encuentra en la aplicación y solicita ingresar un nuevo nombre de grupo
		11.3	Crear un grupo como administrador en la aplicación dejando el campo Nombre del grupo vacío	La aplicación muestra un mensaje de error y solicita ingresar un nombre de grupo de más de un carácter no nulo ni vacío
12	Consultar Grupo	12.1	Consultar un grupo como administrador en la aplicación	La aplicación permite consultar un grupo
		12.2	Consultar un grupo como administrador no existente en la aplicación	La aplicación muestra un mensaje diciendo que el grupo no existe en la aplicación.
		12.3	Consultar un grupo como administrador en la aplicación dejando el campo Nombre del grupo vacío	La aplicación muestra un mensaje de error y solicita ingresar un nombre de grupo de más de un carácter no nulo ni vacío
13	Actualizar Grupo	13.1	Actualizar como administrador un grupo existente en la aplicación	La aplicación permite actualizar la información del grupo
		13.2	Actualizar la información como administrador de un grupo no existente en la aplicación	La aplicación muestra un mensaje de error y solicita ingresar un grupo que se encuentre en el sistema
		13.3	Actualizar la información como administrador de un grupo dejando el campo nombre de grupo en blanco	La aplicación muestra un mensaje de error y solicita ingresar un nombre de grupo que se encuentre en el sistema con ID de usuario de más de un carácter no nulo ni vacío
14	Crear Rol	14.1	Crear un rol como administrador existente en la aplicación	La aplicación permite crear un rol
		14.2	Crear un rol como administrador ya existente en la aplicación	La aplicación muestra un mensaje diciendo que el rol ya se encuentra en la aplicación y solicita ingresar un nuevo nombre de rol
		14.3	Crear un rol como administrador en la aplicación dejando el campo Nombre del rol vacío	La aplicación muestra un mensaje de error y solicita ingresar un nombre de rol de más de un carácter no nulo ni vacío
15	Consultar Rol	15.1	Consultar un rol como administrador existente en la aplicación	La aplicación permite consultar un rol
		15.2	Consultar un rol como administrador no existente en la	La aplicación muestra un mensaje diciendo que el rol no existe en la

			aplicación	aplicación.
		15.3	Consultar un rol como administrador en la aplicación dejando el campo Nombre del rol vacío	La aplicación muestra un mensaje de error y solicita ingresar un nombre de rol de más de un carácter no nulo ni vacío
16	Actualizar Rol	16.1	Actualizar la información como administrador de un rol existente en la aplicación	La aplicación permite actualizar la información del usuario
		16.2	Actualizar la información como administrador de un rol no existente en la aplicación	La aplicación muestra un mensaje de error y solicita ingresar un usuario que se encuentre en el sistema
		16.3	Actualizar la información como administrador de un rol dejando el campo nombre de rol en blanco	La aplicación muestra un mensaje de error y solicita ingresar un nombre de rol que se encuentre en el sistema de más de un carácter no nulo ni vacío
17	Crear Permiso	17.1	Crear un permiso como administrador existente en la aplicación	La aplicación permite crear un permiso
		17.2	Crear un permiso como administrador ya existente en la aplicación	La aplicación muestra un mensaje diciendo que el permiso ya se encuentra en la aplicación y solicita ingresar un nuevo nombre de permiso
		17.3	Crear un permiso como administrador en la aplicación dejando el campo Nombre del rol vacío	La aplicación muestra un mensaje de error y solicita ingresar un nombre de permiso de más de un carácter no nulo ni vacío
18	Consultar Permiso	18.1	Consultar un permiso como administrador existente en la aplicación	La aplicación permite consultar un permiso
		18.2	Consultar un permiso como administrador no existente en la aplicación	La aplicación muestra un mensaje diciendo que el permiso no existe en la aplicación.
		18.3	Consultar un permiso como administrador en la aplicación dejando el campo Nombre del rol vacío	La aplicación muestra un mensaje de error y solicita ingresar un nombre de permiso de más de un carácter no nulo ni vacío
19	Actualizar Permiso	19.1	Actualizar la información como administrador de un permiso existente en la aplicación	La aplicación permite actualizar la información del permiso
		19.2	Actualizar la información como administrador de un permiso no existente en la aplicación	La aplicación muestra un mensaje de error y solicita ingresar un permiso que se encuentre en el sistema
		19.3	Actualizar la información como administrador de un permiso dejando el campo nombre de permiso en blanco	La aplicación muestra un mensaje de error y solicita ingresar un nombre de permiso que se encuentre en el sistema de más de un carácter no nulo ni vacío

20	Crear Tipo Recurso	20.1	Crear un tipo de recurso como administrador existente en la aplicación	La aplicación permite crear un tipo de recurso
		20.2	Crear un tipo de recurso como administrador ya existente en la aplicación	La aplicación muestra un mensaje diciendo que el tipo de recurso ya se encuentra en la aplicación y solicita ingresar un nuevo nombre de tipo de recurso
		20.3	Crear un tipo de recurso como administrador en la aplicación dejando el campo Nombre del rol vacío	La aplicación muestra un mensaje de error y solicita ingresar un nombre de tipo de recurso de más de un carácter no nulo ni vacío
21	Consultar Tipo Recurso	21.1	Consultar un tipo de recurso como administrador existente en la aplicación	La aplicación permite consultar un tipo de recurso
		21.2	Consultar un tipo de recurso como administrador no existente en la aplicación	La aplicación muestra un mensaje diciendo que el tipo de recurso no existe en la aplicación.
		21.3	Consultar un tipo de recurso como administrador en la aplicación dejando el campo Nombre del tipo de recurso vacío	La aplicación muestra un mensaje de error y solicita ingresar un nombre de tipo de recurso de más de un carácter no nulo ni vacío
22	Actualizar Tipo Recurso	22.1	Actualizar la información como administrador del tipo de recurso existente en la aplicación	La aplicación permite actualizar la información del tipo de recurso
		22.2	Actualizar la información como administrador de un tipo de recurso existente en la aplicación	La aplicación muestra un mensaje de error y solicita ingresar un tipo de recurso que se encuentre en el sistema
		22.3	Actualizar la información como administrador de un tipo de recurso dejando el campo nombre de tipo de recurso en blanco	La aplicación muestra un mensaje de error y solicita ingresar un nombre de tipo de recurso que se encuentre en el sistema de más de un carácter no nulo ni vacío
23	Consultar Acción	23.1	Consultar una acción como administrador existente en la aplicación	La aplicación permite consultar una acción
		23.2	Consultar una acción como administrador no existente en la aplicación	La aplicación muestra un mensaje diciendo que la acción no existe en la aplicación.
		23.3	Consultar una acción como administrador en la aplicación dejando el campo Nombre de acción vacío	La aplicación muestra un mensaje de error y solicita ingresar un nombre de acción más de un carácter no nulo ni vacío
24	Agregar Rol a Grupo	24.1	Agregar como administrador un rol a un grupo existente en la aplicación	La aplicación permite agregar a un rol a un grupo
		24.2	Agregar como administrador un rol a un grupo no existente en la aplicación	La aplicación arroja un mensaje de error y solicita ingresar un grupo que exista en la aplicación

25	Agregar Usuario a Grupo	25.1	Agregar como administrador un usuario a un grupo existente en la aplicación	La aplicación permite agregar a un usuario a un grupo
		25.2	Agregar como administrador un usuario a un grupo no existente en la aplicación	La aplicación arroja un mensaje de error y solicita ingresar un grupo que exista en la aplicación
26	Agregar Rol a Usuario	26.1	Agregar como administrador un rol a un usuario existente en la aplicación	La aplicación permite agregar a un rol a un usuario
		26.2	Agregar como administrador un rol a un usuario no existente en la aplicación	La aplicación arroja un mensaje de error y solicita ingresar un usuario que exista en la aplicación
27	Crear Aplicación	27.1	Realizar la creación de una Aplicación con el nombre vacío	El sistema no permitirá crear la aplicación
		27.2	Realizar la creación de una aplicación con el correo vacío	El sistema no permitirá crear la aplicación
		27.3	Realizar la creación de una aplicación ingresando los datos correctos	El sistema permitirá la creación de la aplicación
28	Consultar Aplicación	28.1	Realizar la consulta de una Aplicación	El sistema permitirá consultar la aplicación
		28.2	Realizar la consulta de una aplicación que no exista	El sistema devolverá un mensaje indicando que la aplicación no existe.
		28.3	Realizar la consulta de aplicaciones sin ingresar ningún filtro de búsqueda	El sistema mostrará todas las aplicaciones existentes
29	Actualizar Aplicación	29.1	Ingrese a la información de una aplicación, elimine el correo electrónico y verifique que no permita guardar el cambio	El sistema no permitirá guardar el cambio de la modificación.
		29.2	Ingrese a la información de una aplicación, modifique el check de herencia de otra aplicación.	El sistema verificará la información ingresada y permitirá guardar el cambio.
		29.3	Realice la modificación de toda la información de la aplicación	El sistema verificará la información ingresada y no permitirá realizar la modificación del nombre ni el correo electrónico
		29.3	Realice la modificación de la información de la aplicación	El sistema verificará la información ingresada y permitirá realizar la actualización

3. Evidencias de Ejecución

3	FUNCIONAL	Contacta	Mapa Ubicación: No se visualiza el mapa de ubicación
---	-----------	----------	---



Se ha producido un error.

Esta página no ha cargado Google Maps correctamente. Descubre los detalles técnicos del problema en la consola de JavaScript.